International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وجهود المملكة في مكافحتها

محمد خالد المالكي
باحث ماجستير، تخصص القانون العام، كلية الحقوق، جامعة الملك عبد العزيز، جدة، المملكة العربية السعودية
momalkii@hotmail.com

محمد حميد المزمومي
أستاذ القانون الجنائي، كلية الحقوق، جامعة الملك عبد العزيز، جدة، المملكة العربية السعودية

المستخلص

يهدف هذا البحث إلى دراسة التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وتسليط الضوء على جهود المملكة العربية في مكافحتها، ولما كانت تلك الجريمة مرتبطة ارتباطاً وثيقاً بالجرائم المعلوماتية، ونظراً لحداثة الجرائم المعلوماتية وتطورها الملحوظ في العصر الحديث المرتبط بتطور وانتشار الإنترنت أدى ذلك إلى تنامي خطر الجرائم المعلوماتية بمختلف أنماطها وأنواعها وأشكالها، مما أدى إلى تضافر الجهود الدولية لمكافحة تلك الجرائم والتصدي لذلك التوغل والتفشي في كافة دول العالم. وقد بذلت المملكة العربية السعودية في سبيل مكافحة الجرائم المعلوماتية جهداً ملحوظاً وعملت المملكة على تطوير النظم التشريعية لمواكبة سبل مكافحة كافة الجرائم المعلوماتية.

اتبعت الدراسة المنهج التحليلي لنصوص نظام مكافحة جرائم المعلوماتية السعودي، وكذلك المنهج المقارن في القوانين والنظم التشريعية المماثلة بهدف الوصول إلى النتائج والتوصيات المتعلقة بالدراسة.

وقد تناول البحث بيان مدى تطور النظم التشريعية والجهود المبذولة في مكافحة الجرائم المعلوماتية على المستوى الدولي عموماً وفي المملكة العربية السعودية خصوصاً، ثم تطرق البحث إلى التعريف بالمقصود بجريمة الدخول غير المشروع إلى النظام المعلوماتي، وذلك عبر تقسيم الدراسة إلى مبحثين أساسيين، المبحث الأول تطور النظم التشريعية في مكافحة الجرائم المعلوماتية، وقد تناولته الدراسة من خلال مطلبين هما المطلب الأول نظرة عامة عن الجهود الدولية في مكافحة الجرائم المعلوماتية، والمطلب الثاني تطور جهود المملكة العربية السعودية في مكافحة الجرائم المعلوماتية، أما المبحث الثاني فقد تناولت الدراسة التعريف بجريمة

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

الدخول غير المشروع إلى النظام المعلوماتي، من خلال تقسيمه إلى مطلبين، المطلب الأول مفهوم وفلسفة جريمة الدخول غير المشروع إلى النظام المعلوماتي، والمطلب الثاني التميز بين جريمة الدخول غير المشروع وما يرتبط بها.

الكلمات المفتاحية: الجرائم المعلوماتية، نظام مكافحة جرائم المعلوماتية، الدخول غير المشروع، النظام المعلوماتي، جريمة تجاوز حدود التصريح في النظام المعلوماتي، جريمة البقاء غير المصرح به في النظام المعلوماتي، جريمة التنصت أو الالتقاط للمعلومات في النظام المعلوماتي.

Introduction to the crime of unauthorized access to information systems and the Kingdom's efforts to combat it

Mohammed Khalid Al Malki
Master's Researcher Specializing Public Law, College of Law, King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia
Momalkii@hotmail.com

Mohammed Hamid Al Mazmoumi
Professor of Criminal Law, College of Law, King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia

Abstract

This research aims to study the definition of the crime of unauthorized access to information systems and to highlight the efforts of the Kingdom of Saudi Arabia in combating it. Since this crime is closely related to cybercrimes, and given the novelty and significant evolution of cybercrimes in the modern era with the development and spread of the Internet, the threat of cybercrimes in various forms and types has increased. This has led to a concerted international effort to combat these crimes and address their infiltration and spread in all countries of the world. The Kingdom of Saudi Arabia has made intensive efforts to combat cybercrimes and has worked on

developing legislative systems to keep pace with methods of combating all cybercrimes.

The study adopted an analytical approach to the texts of the Saudi Anti-Cyber Crime Law, as well as a comparative approach to similar laws and legislative systems, aiming to reach conclusions and recommendations related to the study.

The research addressed the extent of the development of legislative systems and the efforts made to combat cybercrimes at the international level in general and in the Kingdom of Saudi Arabia in particular. The research then discussed the definition of the crime of unauthorized access to information systems by dividing the study into two main sections. The first section focused on the development of legislative systems in combating cybercrimes, which the study addressed through two subsections: the first subsection provided an overview of international efforts to combat cybercrimes, and the second subsection discussed the development of the efforts of the Kingdom of Saudi Arabia in combating cybercrimes. The second section dealt with the definition of the crime of unauthorized access to information systems, divided into two subsections: the first subsection covered the concept and philosophy of the crime of unauthorized access to information systems, and the second subsection distinguished between the crime of unauthorized access and related offenses.

Keywords: Cybercrimes, Anti-Cybercrime Law, Unauthorized Access, Information System, Crime of Exceeding Permission Limits in the Information System, Crime of Unauthorized Presence in the Information System, Crime of Eavesdropping or Intercepting Information in the Information System.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

خطة الدراسة

أولاً: المقدمة

الحمد لله رب العالمين والصلاة والسلام على نبينا محمد الصادق الأمين وعلى من تبع هداه بإحسانٍ إلى يوم الدين.

يُعنى هذا البحث في المقام الأول بدراسة التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي، وتسليط الضوء على جهود المملكة العربية في مكافحتها، وبما أن الجريمة مرتبطة ارتباطاً وثيقاً بالجرائم المعلوماتية، فلا يكاد يوجد تشريع خاص في مجال مكافحة الجرائم المعلوماتية إلا ونص على جريمة الدخول غير المشروع إلى النظام المعلوماتي بل ويبتدئ التجريم بهذه الجريمة، نظراً لأهمية تلك الجريمة، فهذه الجريمة تمثل تهدياً حقيقياً وخطيراً للنظم المعلوماتية، فهذه الجريمة تنتهك قواعد الخصوصية الإلكترونية للأفراد، وقد يتعدى الأمر كذلك إلى أسرار الدول وأمنها القومي وعصب اقتصادها ومؤسساتها المالية وقد تصل الخسائر إلى خسائر مالية ومادية ومعنوية قد لا يمكن تعويضها أو إصلاحها.

وقبل البدء في دراسة التعريف بجريمة الدخول غير المشروع في النظام المعلوماتي وجب التطرق إلى الجهود الدولية في مكافحة الجرائم المعلوماتية وصولاً إلى بيان مدى تطور جهود المملكة العربية السعودية في مكافحة الجرائم المعلوماتية. ثم بعد ذلك التطرق إلى التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي من خلال بيان مفهوم وفلسفة جريمة الدخول غير المشروع إلى النظام المعلوماتي ونصل من خلال ذلك التعريف إلى التميز بين جريمة الدخول غير المشروع وما يرتبط بها من جرائم مثل جريمة تجاوز حدود التصريح في النظام المعلوماتي، وجريمة البقاء غير المصرح به في النظام المعلوماتي، وجريمة التنصت أو الالتقاط للمعلومات في النظام المعلوماتي، وبيان أوجه التشابه والاختلاف بينهم.

ثانياً: مشكلة الدراسة

تحاول هذه الدراسة تسليط الضوء على الجهود الدولية المبذولة لمكافحة الجرائم المعلوماتية وخاصة جهود المملكة العربية السعودي في مكافحة الجرائم المعلوماتية في العموم وبيان مدى تطور جهودها في مكافحة جريمة الدخول غير المشروع إلى النظام المعلوماتي على وجه الخصوص على المستويين المستوى الحكومي ومستوى القطاع الخاص، كما تهدف إلى البحث في نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم (م / 17) بتاريخ 1428/3/8 هـ الموافق 2007/3/27 الذي يجرم فعل الدخول غير

المشروع إلى النظام المعلوماتي وذلك من خلال البحث التحليلي لنصوصه للوقوف على التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي للإجابة على الأسئلة الأتية:

1. ما هي الجهود الدولية والتعاون الدولي والعربي في مجال مكافحة الجرائم المعلوماتية وجريمة الدخول غير المشروع؟
2. ما هي جهود المملكة العربية السعودية في مجال مكافحة الجرائم المعلوماتية وجريمة الدخول غير المشروع؟
3. ما تعريف المقصود بالجرائم المعلوماتية وجريمة الدخول غير المشروع إلى النظام المعلوماتي؟
4. ما أوجه التشابه والاختلاف بين جريمة الدخول غير المشروع إلى النظام المعلوماتي وما يشابها أو يرتبط بها؟

ثالثاً: أهداف الدراسة

تهدف الدراسة إلى:

1. الوقوف على مدى التطور الدولي والعربي في جهود مكافحة جريمة الدخول غير المشروع إلى النظام المعلوماتي.
2. الوقوف على مدى التطور في جهود المملكة العربية السعودية في مكافحة جريمة الدخول غير المشروع إلى النظام المعلوماتي في القطاع الحكومي والقطاع الخاص.
3. التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وفلسفة التجريم.
4. بيان أوجه التشابه والاختلاف بين جريمة الدخول غير المشروع وبين ما يشابها ويرتبط بها.

رابعاً: أهمية الدراسة

تكمن أهمية الدراسة في بيان الجهود الدولية والتعاون الدولي والعربي في مكافحة الجرائم المعلوماتية عموماً وجريمة الدخول غير المشروع إلى النظام المعلوماتي خصوصاً والوقوف على مدى تطور جهود المملكة العربية السعودية في مكافحة جريمة الدخول غير المشروع إلى النظام المعلوماتي كما تكمن أهمية الدراسة أيضاً في التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وبيان أوجه التشابه والاختلاف بينها

وبين ما يشابها أو يرتبط بها من جرائم مماثلة، وذلك نظراً لأهمية تلك الجريمة كما بينا سالفاً، فمن الناحية الفنية فجريمة الدخول غير المشروع تعتبر بوابة مرور إجباري لا مناص منها للعبور لارتكاب غيرها من الجرائم الإلكترونية فمعظم الجرائم الإلكترونية تتطلب المرور بجريمة الدخول غير المشروع، ومن الناحية القانونية فجريمة الدخول غير المشروع تعتبر أم الجرائم الإلكترونية.

وأما عن الناحية العلمية فتأتي أهمية الدراسة من حداثة النظم القانونية في صياغة تشريعات مستقلة خاصة بمكافحة الجرائم المعلوماتية، كما أن الجرائم المعلوماتية أصبحت في تزايد مستمر بشكال وأساليب وتقنيات مختلفة وذلك بسب التطور المستمر والدائم في المجال التكنولوجي، مما يوجب على الباحثين في مجال مكافحة الجرائم المعلوماتية مواكبة ذلك التطور بمزيد من الدراسات والأبحاث كلاً في مجاله ومن هنا تكمن أهمية الدراسة في التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وفق أخر المستجدات والتشريعات والنظم القانونية.

وأما عن الناحية العملية فتاتي أهمية الدراسة في نشر الوعي بجهود المملكة العربية السعودية في مكافحة جريمة الدخول غير المشروع وبيان خطورة الجرائم المعلوماتية عموماً وبيان خطورة جريمة الدخول غير المشروع إلى النظام المعلوماتي وبيان التعريف بها وما يشابها.

خامساً: منهج الدراسة

تسلك الدراسة المنهج التحليلي لنصوص نظام مكافحة جرائم المعلوماتية السعودي، وتلجأ الدراسة أيضاً إلى المنهج المقارن في القوانين والنظم التشريعية المماثلة مما يساعد في إثراء الدراسة بهدف الوصول إلى النتائج والتوصيات المتعلقة بمشكلة الدراسة.

سادساً: حدود الدراسة

تعتمد الدراسة في حدودها بشكل أساسي على المملكة العربية السعودية في بيان جهودها المبذولة في مكافحة جريمة الدخول غير المشروع إلى النظام المعلوماتي، وعلى نصوص نظام مكافحة جرائم المعلوماتية السعودي في بيان التعريف بالجريمة.

سابعاً: صعوبات الدراسة

إن أبرز صعوبات الدراسة التي واجهها الباحث تتمثل في قلة المراجع والدراسات والأبحاث المتعلقة بجريمة الدخول غير المشروع إلى النظام المعلوماتي بشكل منفصل ومحدد وفقاً لنصوص نظام مكافحة جرائم المعلوماتية السعودي، ورغم ذلك فقد حاول الباحث الاستناد على المراجع المتاحة واعتمد على المنهج التحليلي لنصوص نظام مكافحة جرائم المعلوماتية السعودي، واستند الباحث أيضاً على المنهج المقارن والاجتهادات الفقهية للتغلب على تلك الصعوبات.

ثامناً: الدراسات السابقة

الدراسة الأولى: محمد الصاعدي، جرائم الإنترنت وجهود المملكة العربية السعودية في مكافحتها، من أعمال ندوات: مكافحة الجريمة عبر الإنترنت – ورشة عمل: أمن المعلومات والتوقيع الإلكتروني، القاهرة: المنظمة العربية للتنمية الإدارية، (2010م). تناولت الدراسة تسليط الضوء على تعريف جرائم الإنترنت، وطبيعة وسمات المجرم المعلوماتي، وتناولت الجهود الدولية في مكافحة جرائم الإنترنت، كما سلطت الدراسة على جهود المملكة العربية السعودية في مكافحة جرائم الإنترنت، ولكن الدراسة لم تتناول التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وجهود المملكة العربية السعودية في مكافحتها بشكل خاص، كما أن حدود البحث يعتمد على كافة جرائم الإنترنت بشكل عام، وهو ما تفردت به دراستنا الحالية.

الدراسة الثانية: عبد الإله محمد سالم النواسية، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، ع 1، س 10، عام (2016). وتناولت الدراسة أهمية تجريم الدخول غير المصرح به، ومحل الجريمة وأركانها، والجرائم المرتبطة بجريمة الدخول غير المصرح به. إلا أن الدراسة لم تتناول الجهود الدولية أو العربية المبذولة لمكافحة الجريمة فضلاً عن جهود المملكة العربية السعودية، وكذلك اعتماد الدراسة بشكل أساسي على المنهج المقارن، إلا أن درستنا اعتمدت بشكل أساسي المنهج التحليلي للتعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وفقاً لنصوص نظام مكافحة جرائم المعلوماتية السعودي.

تاسعاً: خطة الدراسة

المبحث الأول: تطور النظم التشريعية في مكافحة الجرائم المعلوماتية.

المطلب الأول: نظرة عامة عن الجهود الدولية في مكافحة الجرائم المعلوماتية.

المطلب الثاني: تطور جهود المملكة العربية السعودية في مكافحة الجرائم المعلوماتية.

المبحث الثاني: التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي.

المطلب الأول: مفهوم وفلسفة جريمة الدخول غير المشروع إلى النظام المعلوماتي.

المطلب الثاني: التميز بين جريمة الدخول غير المشروع وما يرتبط بها.

تمهيد وتقسيم

تسلط الدراسة الضوء على تطور جهود المملكة العربية السعودية في مكافحة الجرائم المعلوماتية عموماً وجريمة الدخول غير المشروع خصوصاً وتهدف إلى التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وفلسفة تجريمها والتميز بين جريمة الدخول غير المشروع وما يرتبط بها وبيان أوجه التشابه والاختلاف بينهما.

المبحث الأول: تطور النظم التشريعية في مكافحة الجرائم المعلوماتية

يهتم هذا البحث بدراسة جريمة الدخول غير المشروع إلى النظام المعلوماتي ومع ارتباط تلك الجريمة بالجرائم المعلوماتية، ومع حداثة الجرائم المعلوماتية وتطورها الملحوظ مع تطور وانتشار الإنترنت، ساهم كل ذلك إلى تنامي خطر تلك الجرائم المعلوماتية بمختلف أنماطها وأنواعها وأشكالها على جميع دول العالم، مما أدى إلى تضافر الجهود الدولية لمكافحة تلك الجرائم والتصدي لتوغلها وتفشيها في كافة دول العالم كما بينا سالفاً.

لذا بذلت المملكة العربية السعودية في سبيل مكافحة الجرائم المعلوماتية جهداً مكثفاً وعملت المملكة على تطوير النظم التشريعية لمواكبة سبل مكافحة كافة الجرائم المعلوماتية.

وبالتالي يتطلب الأمر قبل الدخول في صلب موضوع البحث بيان تطور النظم التشريعية والجهود المبذولة في مكافحة الجرائم المعلوماتية على المستوى الدولي عموماً وفي المملكة العربية السعودية خصوصاً بغية الوصول إلى مدى تطور النظم التشريعية في مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.

وسنتطرق في هذا المبحث إلى مدى التطور العالمي في نظم مكافحة الجرائم المعلوماتية وصولاً إلى مدى التطور في الجهود المبذولة من قبل المملكة العربية السعودية في مكافحة الجرائم المعلوماتية وذلك وفق ما يلي:

المطلب الأول: نظرة عامة عن الجهود الدولية في مكافحة الجرائم المعلوماتية.

المطلب الثاني: تطور جهود المملكة العربية السعودية في مكافحة الجرائم المعلوماتية.

المطلب الأول: نظرة عامة عن الجهود الدولية في مكافحة الجرائم المعلوماتية

تكمن اختصاص هذه الدراسة ببحث جريمة الدخول غير المشروع إلى النظام المعلوماتي دون غيرهم، إلا أنه نظراً لكون ظهور هذه الجريمة مرتبطاً ارتباطاً وثيقاً مع التطور التكنولوجي المتزايد والمستمر في أنظمة تقنية المعلومات، ومع اتساع استخدام الإنترنت في كافة دول العالم الذي أدى إلى انتشار البيانات والمعلومات بصورة واسعة، جعلت من المجرمين ينظرون إلى ذلك التطور بأنه ملاذاً لجرائمهم وبيئة خصبه من أجل الاستيلاء على البيانات والمعلومات المتواجدة على شبكة الإنترنت مما أدى إلى ظهور ما يعرف بالجرائم المعلوماتية (Information Crimes) والتي تعددت صورها وأشكالها وأنواعها وكانت جريمة الدخول غير المشروع إلى النظام المعلوماتي هي إحدى أنواعها.

ومن هنا يجب الإشارة إلى خطورة الجرائم المعلوماتية وجرائم الإنترنت عموماً فهي أكثر خطورة من الجرائم التقليدية، نظراً لأن ضررها لا يقتصر فقط على الأفراد بل قد ينتشر ليشمل المجتمعات والحكومات والمؤسسات وقد يكون الصعيدين الدولي والمحلي. كما أن حجم تلك الجرائم وخطورتها وارتفاع حجم الخسائر الناتجة عنها يتسع ويزداد طردياً مع التطور التكنولوجي المتزايد ومع عدم وجود أنظمة وقوانين موحدة بين كافة دول العالم لمكافحة تلك الجرائم. [1]

في عام 1981م، على سبيل المثال كانت من أوائل الجرائم المعلوماتية المسجلة ما قامت مجموعة من الألمان مما كان لهم توجه سياسي راديكالى وكانت لديهم معرفة قوية بالكمبيوتر واستخدامات التكنولوجيا وقاموا بتشكيل نادي شاس (Chaos) للكمبيوتر بألمانيا وقد تمكنوا من الدخول غير المشروع لمكتب بريد

[1] الصاعدي، محمد، "جرائم الإنترنت وجهود المملكة العربية السعودية في مكافحتها." في أعمال ندوات: مكافحة الجريمة عبر الإنترنت – ورشة عمل: أمن المعلومات والتوقيع الإلكتروني، القاهرة: المنظمة العربية للتنمية الإدارية، (2010م)، ص (4). مسترجع من http://search.mandumah.com/Record/125041

من خلال اختراق ثغرة أمنية. وقاموا بتحويل أموال بمبالغ طائلة منه ورغم أنهم سرعان ما أعادوا الأموال إلا أنهم قاموا بالإدلاء ببيان ينتقد الحكومة فيما يتعلق بالإجراءات الغير فعالة لمكافحة جرائم النظم المعلوماتية والأمن المعلوماتي[2].

إن من أوائل الدول التي كان لها السبق في سن قانون لمكافحة الجرائم المعلوماتية هي دولة السويد فقد صدر قانون البيانات السويدي عام 1973 م. واختص بمكافحة العديد من قضايا الجرائم المعلوماتية من أهمها الاحتيال من خلال الحاسب الآلي وكذلك شمل القانون السويدي نصوص خاصة بجرائم الدخول غير المشروع على البيانات والنظم المعلوماتية. ومن ثم تعاقبت النظم التشريعية الدولية في مكافحة الجرائم المعلوماتية. فلحقت الولايات المتحدة الأمريكية بالركب خلف دولة السويد ففي الفترة من عامي (1976 – 1985) سنت الولايات المتحدة العديد من القوانين المتعلقة بمكافحة الجرائم المعلوماتية.

وجاءت كندا لتلحق بركاب التطور في نظم مكافحة الجرائم المعلوماتية بتعديل قانونها الجنائي في عام 1985م، وقد شمل مواد خاصة بجرائم النظم المعلوماتية منها مواد متعلقة بجرائم الدخول غير المشروع للأنظمة المعلوماتية، وفي عام 1988، عملت فرنسا على تطوير القانون الجنائي الخاص بها ليتم إضافة جرائم النظم المعلوماتية. [3]

وأما عن الدولة العربية، فعلى الرغم أنها لم تكن بمنأى عن هذا التطور العالمي في نظم مكافحة الجرائم المعلوماتية إلا أنه كانت لفترة طويلة أغلب الدول العربية تطبق القواعد العامة للقانوني الجزائي على جرائم النظم المعلوماتية إلا أن قامت الدول العربية بمواكبة ومسايرة التطور الهائل والملحوظ في الأنشطة الإجرامية المتعلقة بالنظم المعلوماتية والتكنولوجية من خلال إصدار القوانين والنظم والتشريعات الخاصة بمكافحة جرائم تقنية المعلومات ومن أبرز تلك الدول:

- المملكة العربية السعودية التي جاءت على قائمة أولى الدول العربية حيث أصدرت نظام مكافحة جرائم المعلوماتية حيث صدر بقرار رئيس مجلس الوزراء رقم 79 بتاريخ 1428/3/7 هـ. وصدق عليه بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ. الموافق 2007/3/27 م.

[2] Goshua (B.hill) , nancy (E. MARION) , Introduction to Cybercrime: Computer Crimes Laws, and Policing in the 21st Century , PUBLISHED IN PRAEGER SECURITY INTERNATIONAL , USE , 2016 , CHAPTER 2 .P .2.

[3] المراغي، أحمد عبد اللاه، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها –دراسة تحليلية تأصيلية مقارنة -، بحث مُقدَم إلى المؤتمر العلمي العاشر لكلية الحقوق جامعة أسيوط، عنوان المؤتمر (العصر الرقمي وإشكالياته القانونية)، في الفترة من 5-6 أبريل لسنة 2016م)، ص (53-54).

- دولة الإمارات العربية المتحدة أقرت مرسوم بقانون رقم (5) لسنة 2012 الخاص بمكافحة جرائم تقنية المعلومات.
- دولة قطر أصدرت قانون رقم (4) لسنة 2014 م لمكافحة الجرائم الإلكترونية.
- دولة جمهورية مصر العربية أصدرت القانون رقم 175 لسنة 2018 م بشأن مكافحة جرائم تقنية المعلومات.
- دولة فلسطين حيث صدر القانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية.

ورغم التطور الهائل للنظم التشريعية في مكافحة الجرائم المعلوماتية على مستوى كافة دول العالم في تشريعاتها الوطنية. إلا أنه لا جدل أن من أكبر الصعوبات التي تواجه نظم مكافحة الجرائم المعلوماتية في العصر الحديث هو الاختلاف في نصوص تلك التشريعات الوطنية من دولة لأخرى "سنبين ذلك لاحقاً في الفصول القادمة".

إن التطور الهائل لتكنولوجيا المعلومات في العصر الحالي أدى إلى تزايد حجم الجرائم المعلوماتية في كافة دول العالم وجعل من تلك الجرائم ومرتكبيها جرائم ذات طابع دولي كون مرتكبي الجرائم المتعلقة بالنظم المعلوماتية يستغل الاختلاف في تلك التشريعات ومع قدرتهم على ارتكاب تلك الجرائم عبر الدول المختلفة التي قد تكون خطرها أقل من غيرها في نطاق مكافحة جرائم النظم المعلوماتية أدى ذلك إلى جعل المجتمع الدولي يتأثر بتلك الجرائم بشكل ملحوظ مما أوجد الحاجة إلى نظم وقوانين وتشريعات دولية لمكافحة جرائم النظم المعلوماتية.

إن المخاطر والتحديات في مكافحة جرائم النظم المعلوماتية تظهر الحاجة الملحة إلى الموازنة بين السيادة الوطنية وتنسيق الجهود الدولية في سبيل مكافحة الجرائم المعلوماتية ومع تدارك الدول العالمية لتلك التحديات وفي سبيل تحقيق المصلحة العليا الدولية للمواطنين فقد تم إبرام العديد من الاتفاقيات الدولية في سبيل مكافحة الجرائم المعلوماتية منها الاتفاقيات العربية ومنها الاتفاقيات الدولية. [4]

وسوف نلقي نظرة عامة عن تلك الجهود الدولية المبذولة في مجال مكافحة الجرائم المعلوماتية، من خلال تقسيم ذلك المطلب إلى فرعين أساسين يتمثلان فيما يلي:

[4] المطيري، خالد ظاهر محمد، مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية، (الكويت: أكاديمية سعد العبد الله للعلوم الأمنية، 2020م.)، ص (42-43).

الفرع الأول: الاتفاقية العربية لمكافحة جرائم النظم المعلوماتية.

الفرع الثاني: الاتفاقيات الدولية لمكافحة جرائم النظم المعلوماتية.

الفرع الأول: الاتفاقية العربية لمكافحة جرائم النظم المعلوماتية

وقع وزراء العرب من وزارتي الداخلية والعدل على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات عام 2010 م بتاريخ (23/ 2010/12م) على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وكانت تلك الاتفاقية بمثابة أهم الاتفاقيات التي جاءت كنتيجة للجهود المضنية التي قامت بها جامعة الدول العربية لمواجهة جرائم النظم المعلوماتية في الدول العربية وذلك ضمن إطار قانوني ونظامي يدعم التدابير الأمنية لمكافحة الجرائم المتعلقة بتقنية المعلومات. [5]

وجاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من خمسة فصول وتشمل ثلاث وأربعون مادة.

واحتوى الفصل الأول بين طياته الأحكام العامة منها الهدف من الاتفاقية، وتعريف المصطلحات التي تحتويها الاتفاقية، ومجالات تطبيق الاتفاقية، وتطرق الفصل الأول في مادته الرابعة إلى مبدأ صون السيادة لدول الاتفاقية.

وأما الفصل الثاني فقد جاء بين طياته المواد الخاصة بالتجريم في الاتفاقية، وتناولت المواد (من المادة (الخامسة إلى المادة الحادية والعشرون) كافة الأمور المتعلقة بالتجريم في النظم المعلوماتية وألزمت المادة الخامسة من الاتفاقية كل دولة طرف في الاتفاقية بتجريم كافة الأفعال المبينة بذلك الفصل في الاتفاقية وجاءت المادة السادسة من الاتفاقية بتجريم الدخول غير المشروع كما نوهت الاتفاقية على ضرورة تشديد عقوبة جريمة الدخول غير المشروع في حالتين:

أولاً: إذا ترتب على هذا الدخول أو الاستمرار أو الاتصال أو البقاء بهذا الاتصال محو أو تشويه أو تعديل أو تدمير أو نقل أو نسخ للبيانات الموجودة أو المحفوظة وكذلك لأجهزة أو الأنظمة الإلكترونية وكذلك شبكات الاتصال وإلحاق الضرر بالمستفيدين وبالمستخدمين.

ثانياً: الحصول على معلومات حكومية سرية.

[5] الغياثين، محمد حمد عمر، الجرائم المعلوماتية عابرة الحدود-دراسة مقارنة-قدمت لنيل درجة الدكتوراه في كلية الحقوق جامعة القاهرة، عام (2013م)، ص (65).

وقد عنيت الاتفاقية العربية كذلك بمواجهة عدة جرائم ألزمت من خلالها الدول العربية بإدخال تعديلات على تشريعاتها الخاصة لتجريم تلك الأفعال الخاصة بمكافحة جرائم النظم المعلوماتية وكما تناولت أيضاً في مادتها التاسعة عشر مفهوم الشروع والاشتراك في كافة الجرائم المذكورة في الفصل الثاني من الاتفاقية وختمت الاتفاقية فصلها الثاني بالمادتين العشرون والحادية والعشرون من الاتفاقية وتناولت من خلالهما المسئولية الجنائية للأشخاص الطبيعية والمعنوية وكذلك تفردت الاتفاقية في مادتها الحادية والعشرون وتناولت تشديد العقوبات على كافة الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات. ولقد جاء تلك الجرائم في مواد الاتفاقية في فصلها الثاني في المواد (من المادة السادسة إلى المادة التاسعة عشر) على النحو التالي: [6]

1. جريمة الدخول غير المشروع.
2. جريمة الاعتراض غير المشروع.
3. الاعتداء على سلامة البيانات.
4. جريمة إساءة استخدام وسائل تقنية المعلومات.
5. جريمة التزوير الخاصة بالنظم المعلوماتية.
6. جريمة الاحتيال الخاصة بالنظم المعلوماتية.
7. جريمة الإباحية وما يرتبط بها مثل المقامرة والاستغلال الجنسي الخاصة بالنظم المعلوماتية.
8. جريمة الاعتداء على حرمة الحياة الخاصة المتعلقة بالنظم المعلوماتية.
9. الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات.
10. الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة الخاصة بالنظم المعلوماتية.
11. الاستخدام غير المشروع لأدوات الدفع الإلكترونية.
12. الشروع والاشتراك في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من الاتفاقية.

[6] د/ القاضي، رامي متولي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، الطبعة الأولي، عام 2011 ص (70-71).

ولقد اهتمت أيضاً الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في فصلها الثالث بكافة الأحكام الإجرائية المطلوبة في نطاق تطبيق الاتفاقية وذلك في المواد (من المادة الثانية والعشرون إلى المادة التاسعة والعشرون) وأما عن الفصل الرابع من الاتفاقية جاء في المواد (من المادة الثلاثون إلى المادة الثالثة والأربعون) فقد تناولت الاتفاقية محور التعاون القانوني والقضائي بين الدول العربية لمكافحة جرائم تقنية المعلومات والنظم المعلوماتية.

وخُتمت الاتفاقية بالفصل الخامس الذي تناول بعض الأحكام الختامية الخاصة بإجراءات وضع الاتفاقية موضع التنفيذ.

الفرع الثاني: الاتفاقيات الدولية لمكافحة جرائم النظم المعلوماتية

من المسلم به أن الجرائم المعلوماتية هي جرائم عابرة للحدود وتؤثر نتائج تلك الجرائم على المجتمع الدولي بوجه عام بشكل مباشر كون أن الجرائم المعلوماتية تتم عبر الإنترنت وتخترق حدود الدول ويجعل من الصعب تنظيمها أو مراقبتها أو تعقبها دون تنسيق دولي لذا يعتبر التنسيق الدولي لمكافحة الجرائم المعلوماتية أمر في غاية الأهمية كون أن هذه الجرائم ذات طابع خاص ولا تحدها حدود فهي جرائم عابرة للحدود.

ولقد اتخذت الجهود الدولية المبذولة في مجال مكافحة الجرائم المعلوماتية العديد من الصور من اتفاقيات ومؤتمرات وقرارات ومعاهدات، كما كان أيضاً لمؤسسات الملكية الفكرية والمؤسسات المالية الدولية والشركات العالمية دوراً بارزاً في تحقيق الحماية الإلكترونية للتجارة الإلكترونية. [7]

وكانت من أهم الجهود المبذولة في مكافحة الجرائم المعلوماتية على المستوى الدولي الجهود التي قامت بها كلاً من منظمة الأمم المتحدة، جهود المنظمة العالمية للملكية الفكرية الويبو [8] والتجارة العالمية، قانون الأونسيترال [9] النموذجي بشأن التجارة الإلكترونية لعام 1996 م، اتفاقية بودابست لمكافحة الجرائم

[7] الجنبيهي، منير محمد، والجنبيهي، ممدوح محمد، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامي، ص (96).
[8] المنظمة العالمية للملكية الفكرية هي إحدى الوكالات المتخصصة التابعة للأمم المتحدة وتختص بالملكية الفكرية ولقد تأسست في 1967/7/14، ودخلت حيز التنفيذ سنة 1970م.
[9] لجنة الأمم المتحدة للقانون التجاري الدولي تم إنشائها بموجب قرار الجمعية العامة للأمم المتحدة بالقرار رقم 22055 (د-21) المؤرخ 1966/12/17. وهي هيئة قانونية تتبع منظمة الأمم المتحدة مختصة بمجال القانون التجاري الدولي.

المعلوماتية، وغيرها الكثير من الجهود الدولية التي عملت على مكافحة الجرائم المعلوماتية كلاً حسب اختصاصه ومجاله واهتماماته.

لقد قامت منظمة الأمم المتحدة بدور بارز لمكافحة الجرائم المعلوماتية ومن أهم تلك الجهود مؤتمر الأمم المتحدة السابع في ميلانو بدولة إيطاليا لمناقشة سبل منع الجريمة ومعاملة المجرمين وقد توجت تلك الجهود بالخروج بعدة مبادئ في مجال مكافحة الجرائم المعلوماتية منها على سبيل المثال التأكيد على ضرورة اتخاذ التدابير الملائمة لحالات الدخول غير المشروع واختراق الخصوصية عن طريق الاطلاع على البيانات والمعلومات المخزنة على نظم الحسابات الآلية، كما أكدت تلك المبادئ على ضرورة تشجيع التشريعات الحديثة لمكافحة جرائم الحاسب الآلي وقد نالت تلك المبادئ استحان دولي وفي عام 1990 تمت المصادقة على تلك المبادئ في هافانا بدولة كوبا. [10]

لقد ساهمت أيضاً جهود المنظمة العالمية للملكية الفكرية ومنظمة التجارة العالمية في مكافحة الجرائم المعلوماتية ومن أبرز تلك الجهود ما قامت به منظمة الويبو من تبني نصوص تشريعية لحماية برامج الحاسب الآلي فقامت بإعداد نصوص نموذجية من أجل مساعدة الدول على استكمال تشريعاتها المستقلة في مجال حماية البرامج الإلكترونية. [11] كما تضافرت معها جهود منظمة التجارة العالمية في محاربة كل ما هو يشكل نسخ وتقليد للبرامج حيث أجازت لمنتجي البرامج ومبدعيها حقوق أصلية دعت البلدان الأعضاء وغير الأعضاء إلى احترامها ومن ذلك تكون منظمة التجارة العالمية قد التزمت بحماية برامج الحاسب الآلي من القرصنة والدخول غير المشروع لها شانها في ذلك شأن المنظمة العالمية للملكية الفكرية. [12]

وفي مجال التجارة الإلكترونية جاء اعتماد لجنة الأمم المتحدة لقانون الأونسيترال النموذجي بشأن التجارة الإلكترونية لعام 1996 م حيث يعتبر ذلك القانون من أهم الجهود الدولية لمكافحة جرائم الإنترنت والجرائم المعلوماتية في مجال التجارة الدولية الإلكترونية منا اهتم القانون النموذجي بشأن التجارة الإلكترونية أن يكون نموذجاً تقتدي به الدول لتحسين قوانينها وتشريعاتها وممارستها لمواجهة التطور البارز في مجال التجارة الإلكترونية وأهمها تطور التقنيات الحاسوبية والنظم الإلكترونية والمعلوماتية وما لحقها من تطور في الجرائم المعلوماتية.

[10] الأمين، محمد، وعبد الحميد، محسن، معاير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة، أكاديمية نايف العربية للعلوم الأمنية، الرياض ط1، عام 1998م. ص (19).
[11] حسام، محمد، ولطفي، محمود، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر القاهرة ط1، عام 1978 ص (161).
[12] الدعجة، أمجد حسن مرشد، استراتيجية مكافحة الجرائم المعلوماتية، (السودان: جامعة أم درمان، رسالة ماجستير، عام 2014)، ص (56-57).

وأما في مجال الاتفاقيات الدولية وبسبب عدم وجود تشريع دولي ملزم بشكل كامل بمكافحة الجرائم الإلكترونية والمعلوماتية بصفة عامة فقد قامت الدول الأوربية بفتح باب التوقيع على اتفاقية بودابست الدولية في 2001/11/23م. لتصبح أولى الاتفاقيات الدولية التي اتجهت لتجريم جميع أشكال الجرائم الإلكترونية ولا سيما الجرائم المعلوماتية. [13]

ولقد تشكلت اتفاقية بودابست الأوربية من أربعة أبواب شملت ثمان وأربعون مادة. لتصبح أول الاتفاقيات الدولية التي اتجهت لتجريم جميع أشكال الجرائم الإلكترونية ولا سيما الجرائم المعلوماتية وتُعد هذه الاتفاقية من أوائل الاتفاقيات التي تصدت لجريمة الدخول غير المشروع.

فقد تناولت الاتفاقية في بابها الأول التعريفات والمصطلحات الخاصة بالاتفاقية، أما عن الباب الثاني ففي القسم الأول منه في المواد من (المادة الثانية إلى المادة السادسة) حيث ناقشت الاتفاقية فيه الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر حيث تناولت المادة الثانية تأكيد على ضرورة اعتماد كل دولة طرف في الاتفاقية باتخاذ ما يلزم من تدابير لتجريم فعل الدخول غير المشروع، وكذلك نوهت المادة الثالثة على مثل هذه التدابير فيما يخص جريمة الاعتراض غير المشروع وأما المادة الرابعة فقد عنيت بجريمة التدخل في البيانات، وأما عن المادة الخامسة والسادسة فقد أولت اهتمامها بجرائم التدخل في النظام وإساءة استخدام الأجهزة.

وأما عن الفصل الثاني من الباب الثاني في الاتفاقية في المواد من (المادة السابعة إلى المادة الثامنة) قد تناولت اتفاقية بودابست الأوربية الجرائم ذات الصلة بالكمبيوتر، وبالفصل الثالث من الباب الثاني في المادة التاسعة فقد عنيت الاتفاقية بالجرائم ذات الصلة بالمحتوى وبالفصل الرابع في المادة العاشرة، فقد خصصته الاتفاقية للجرائم ذات الصلة والمتعلقة بحقوق النشر والتأليف والحقوق ذات الصلة وبالفصل الخامس والأخير من الباب الثاني في المواد من (المادة الحادية عشر إلى المادة الثالثة عشر)، فقد أولت الاتفاقية اهتمامها بالمسؤولية الإضافية مثل المحاولة والتحريض والمساعدة لارتكاب أي من الجرائم المذكورة بالاتفاقية بالإضافة إلى الإشارة إلى ضرورة اتخاذ الدول الأطراف ما يلزم من تدابير تشريعية لضمان مسألة الشركات والأشخاص الاعتباريين عن ارتكاب أي من الجرائم المذكورة بالاتفاقية، وفي ختام الفصل الخامس

[13] عبد الحفيظ، أيمن، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة بأكاديمية مبارك، العدد الخمس والعشرون، يناير 2004م، ص (389).

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

من القسم الأول من الباب الثاني فقد أشارت الاتفاقية إلى ضرورة فرض العقوبات الفعالة والرادعة للجرائم المعلوماتية وكافة الجرائم المنصوص عليها في المواد من المادة (الثانية إلى المادة الحادية عشر) من الاتفاقية.

أما عن القسم الثاني من الباب الثاني من الاتفاقية فقد تناولت فيه الاتفاقية القانوني الإجرائي لها من خلال خمسة فصول تناولت فيهم المواد من (المادة الرابعة عشر إلى المادة الثانية والعشرون) وأما عن الباب الثالث فقد خصصته الاتفاقية إلى المبادئ العامة بالتعاون الدولي لمكافحة الجرائم المعلوماتية من خلال المواد (من المادة الثالثة والعشرون إلى المادة الخامسة والثلاثون) وخُتمت الاتفاقية بالباب الرابع في المواد (من المادة السادسة والثلاثون إلى المادة الثامنة والأربعون) الخاص بالأحكام الختامية للاتفاقية. [14]

المطلب الثاني: تطور جهود المملكة العربية السعودية في مكافحة الجرائم المعلوماتية

سايرت المملكة العربية السعودية التطور الدولي في مجال مكافحة الجرائم المعلوماتية واستفادت من تجارب الدول العربية والأجنبية في التصدي للجرائم المعلوماتية سواء بالطرق الفنية أو القانونية، وعملت المملكة العربية السعودية من اللحظة الأولى لدخول الإنترنت بالمملكة في عام (1999م.) على تطوير وتحديث الأنظمة التشريعية واللوائح والقوانين المتعلقة بمجال مكافحة الجرائم المعلوماتية بما يتناسب مع طبيعة المملكة العربية السعودية من وضعها وسياستها ومكانتها الإسلامية بين دول العالم وكانت تلك الجهود المبذولة على كافة المستويات سواء المستوى الحكومي أو مستوى الأفراد والقطاع الخاص[15].

وسوف نلقي نظرة عامة عن تطور تلك الجهود المبذولة من المملكة العربية السعودية في مجال مكافحة الجرائم المعلوماتية، من خلال تقسيم ذلك المطلب إلى فرعين أساسين يتمثلان فيما يلي:

الفرع الأول: الجهود المبذولة من القطاع الحكومي.

الفرع الثاني: الجهود المبذولة من القطاع الخاص.

الفرع الأول: الجهود المبذولة من القطاع الحكومي

بذل القطاع الحكومي في المملكة جهداً فعالاً في مجال مكافحة الجرائم المعلوماتية ومن أبرز تلك الجهود ما يلي:

[14] للمزيد حول الاتفاقية، عبد اللاه، هلالي، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها أ.د. هلالي عبده اللاه أحمد، أستاذ القانون الجنائي كلية الحقوق، جامعة أسيوط، القاهرة دار النهضة العربية ط8 يناير 2011م.

[15] الصاعدي، محمد، جرائم الإنترنت وجهود المملكة العربية السعودية في مكافحتها، (القاهرة: المنظمة العربية للتنمية الإدارية، 2010)، ص (27).

International Journal of Financial, Administrative and Economic Sciences, London Vol (3), No (10), 2024
https://doi.org/10.59992/IJFAES.2024.v3n10p2 E-ISSN 2977-1498

1. إنشاء وحدات خدمات الإنترنت بمدينة الملك عبد العزيز للعلوم والتقنية للإشراف على نقطة الارتباط بالإنترنت حيث صدر بناءً على قرار مجلس الوزراء رقم (163) بتاريخ 24 / 10 / 1417 هـ. وكانت من أهم مهام تلك الوحدات بجانب تقديم وتطوير خدمات الإنترنت للجهات الحكومية والمستخدمين بالمملكة العربية السعودية أنها تقوم بإعداد اللوائح والأنظمة التي تتعلق بأمان استخدام الإنترنت كما تهتم أيضاً الوحدات بنشر الوعي لضمان الاستخدام الأمن لمستخدمين الإنترنت بالمملكة، ويعتبر من أهم الجهود التي قامت بها تلك الوحدات في مجال مكافحة جرائم الإنترنت هي حجب المواقع الإباحية التي تتنافي مع الدين الحنيف ومع الأنظمة واللوائح المعمول بها بالمملكة.
2. تكوين لجنة أمنية دائمة للإنترنت بهدف الضبط الأمني للمعلومات عبر الإنترنت التي تتنافي مع الأنظمة المعمول بها بالمملكة والسعي لمكافحة الجرائم المعلوماتية بالطرق الممكنة.
3. صدور قرار مجلس الوزراء رقم (229) بتاريخ 1425/8/13 هـ. والذي تضمن نقل كافة مهام وحدات خدمات الإنترنت بمدينة الملك عبد العزيز إلى هيئة الاتصالات وتقنية المعلومات، حيث تولت الهيئة منذ أنشائها وتكليفها بمهامها بجهود مضنية في سبيل مكافحة الجرائم المعلوماتية ومن أهم مشاريعها العمل على تنفيذ وتطوير الهيكل التنظيمي لمشروع مكافحة الرسائل الاقتحامية مثل Spam – Anti من خلال وضع ضوابط للحد منها وذلك بهدف الحد من انتشار الرسائل الاقتحامية وضمان قدرة المؤسسات التجارية ذات المنتجات والخدمات المشروعة على الاستمرار في استخدام الرسائل الإلكترونية بأمان لتقديم خدمات التجارة الإلكترونية [16]. كما تم إنشاء "المركز الوطني للتصديق الرقمي داخل الهيئة بهدف الوصول لمنظومة أمنية متكاملة للحفاظ على سرية المعلومات والتثبت من هوية المتعاملين والمستخدمين وذلك لمنع الدخول غير المشروع. بالإضافة إلى إنشاء "المركز الوطني الإرشادي لأمن المعلومات" في الهيئة بهدف رفع مستوى الوعي بأمن المعلومات في المملكة ونشر سبل الوقاية من تجنب تهديدات الجرائم المعلوماتية.
4. تنظيم المؤتمرات والندوات وورش العمل التي تختص بمناقشة الجرائم المعلوماتية وسبل مكافحاتها ومنها على سبيل المثال "المنتدى السعودي الثاني لأمن المعلومات عام (2005م) والتي نظمته رئاسة الحرس الوطني السعودي في الرياض، ندوة المجتمع الأمن السنوية بعنوان "الظاهرة الإجرامية المعاصرة: الاتجاهات والسمات في الدورة الرابعة عام (2005م) والتي نظمتها كلية الملك فهد الأمنية

[16] الصاعدي، محمد، مرجع سابق، ص (29).

بالرياض، المؤتمر الوطني للتعاملات الإلكترونية (2007م) في الرياض، مؤتمر تقنية المعلومات والأمن الوطني (2007م) والتي نظمته رئاسة الاستخبارات العامة في الرياض. وغيرها الكثير من المؤتمرات والفاعليات وذلك بهدف التوعية بنشر ثقافة الأمن المعلوماتي والتصدي ومكافحة الجرائم المعلوماتية.

5. قيام المملكة العربية السعودية بإقرار نظام مكافحة جرائم المعلوماتية في المملكة، الصادر بالمرسوم الملكي رقم (م/ 17) بتاريخ 1428/3/8 هـ الموافق 2007/3/27 م. والذي يهدف للحد من وقوع الجرائم المعلوماتية وتقرير العقوبات الرادعة لها والذي صنع تناغم بين جميع مؤسسات المملكة كونه تتولى المحكمة المختصة بإيقاع العقوبات أو الإعفاءات الواردة بالنظام وذلك وفق المادة (الحادية عشر) من نظام مكافحة جرائم المعلوماتية، كما تتولى "هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل الضبط والتحقيق وأثناء المحاكمة وذلك وفق المادة (الرابعة عشر) من نظام مكافحة جرائم المعلوماتية. كما تتولى هيئة التحقيق والادعاء العام" مهمة التحقيق والادعاء في الجرائم الواردة بالنظام وذلك وفق المادة (الخامسة عشر) من نظام مكافحة جرائم المعلوماتية.

6. قيام المملكة العربية السعودية بإقرار نظام التعاملات الإلكترونية في المملكة، الصادر بالمرسوم الملكي رقم (م/ 18) بتاريخ 1428/3/8 هـ الموافق 2007/3/27 م. والذي يهدف لضبط التعاملات والتوقيعات الإلكترونية، في إطار نظامي يضفي الثقة والأمان للسجلات الإلكترونية. [17]

الفرع الثاني: الجهود المبذولة من القطاع الخاص

ورغم استمرار الجهود المبذولة من القطاع الحكومي في مكافحة الجرائم المعلوماتية إلا أنه هناك العديد من الجهود المبذولة من القطاع الخاص وقطاع الأفراد والمؤسسات سواء الأهلية أو الخاصة ومن أبرز تلك الجهود ما يلي:

1. إنشاء جمعية الحاسبات السعودية وهي تعتبر أول جمعية غير ربحية تهدف تقديم الأنشطة والبحوث العلمية في مجال علوم الحاسب وتقنية المعلومات.

[17] الصاعدي، محمد، مرجع سابق، ص (30-32).

2. تقديم خدمات "الشبكة الخضراء Green Net" من خلال شركات مزودي خدمة الإنترنت كخدمة اختيارية تهدف لتقديم حماية للأفراد والأسر من المستخدمين الراغبين في استخدام إنترنت نقي ومفلتر من المواقع والصفحات الغير متوافقة مع النظم والمعايير الدينية والأخلاقية المعمول بها بالمملكة.
3. إنشاء مركز خدمة (رقيب) ويعتبر أول مركز أمني لإدارة أمن المعلومات بالمملكة العربية السعودية وتم إطلاقه عام (2008م) حيث يقدم خدمات عديدة منها أنظمة منع التطفل والدخول غير المشروع على الأنظمة المعلوماتية وكذلك خدمات إدارة الثغرات الأمنية ومخاطر أمن المعلومات وغيرها من الخدمات المتعلقة بمكافحة الجرائم المعلوماتية من خلال الوقاية المسبقة وتقديم العلاج السريع والفعال للحفاظ على أمن المعلومات في حال وقوعها.
4. شركة ريثون العربية السعودية وهي شركة سعودية متخصصة بأنظمة الدفاع والفضاء والأمن السبراني والتي تأسست بموجب اتفاقية تعاون بين شركة ريثون الأمريكية ومع الشركة السعودية للصناعات العسكرية وتهدف إلى تقديم كافة الخدمات المتعلقة بالأمن السيبراني ومكافحة الجرائم المعلوماتية وتقديم كذلك العديد من الدورات التدريبية لتطوير ذلك المجال. وتسعى شركة "أرامكو السعودية" بالتعاون مع شركة ريثون العربية السعودية لإطلاق مشروع مشترك لتطوير وتقديم خدمات مكافحة الجرائم المعلوماتية والأمن السيبراني. [18]

المبحث الثاني: التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي

يهتم هذا البحث في المقام الأول بدراسة جريمة الدخول غير المشروع إلى النظام المعلوماتي ولما كانت التشريعات والنظم القانونية لا يكاد يوجد تشريع خاص في مجال مكافحة الجرائم المعلوماتية إلا ونص على تلك الجريمة، وذلك الأمر لم يكن عفوياً وإنما له دلالات قانونية وفنية نظراً لأهمية تلك الجريمة، فمن الناحية الفنية فجريمة الدخول غير المشروع تعتبر بوابة مرور إجباري لا مناص منها للعبور لارتكاب غيرها من الجرائم الإلكترونية فمعظم الجرائم الإلكترونية تتطلب المرور بجريمة الدخول غير المشروع، ومن الناحية القانونية فجريمة الدخول غير المشروع تعتبر أم الجرائم الإلكترونية. وتمثل هذه الجريمة تهدياً

[18] د: عبد الرازق، رانا مصباح عبد المحسن (أستاذ القانون الجنائي المساعد بقسم القانون – الكلية التطبيقية-جامعة الأميرة نورة بنت عبد الرحمن)، آليات مكافحة الجرائم السبرانية في المملكة العربية السعودية "دراسة تحليلية" المجلة القانونية (مجلة متخصصة في الدراسات القانونية) " :ISSN 0758 – 2537" ص (1390).

حقيقياً للنظم المعلوماتية، فهذه الجريمة تنتهك الخصوصية الإلكترونية للأفراد، وقد يتعدى الأمر كذلك إلى أسرار الدولة وأمنها واقتصادها ومؤسساتها المالية وقد تصل الخسائر الى خسائر مالية ومعنوية. [19]

وقبل البدء في دراسة جريمة الدخول غير المشروع في النظام المعلوماتي من حيث الأركان والعقوبات وجب التطرق في هذا المبحث إلى التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي وبيان المقصود بجريمة الدخول غير المشروع وكذلك مفهوم النظم المعلوماتية وصولاً إلى فلسفة التجريم للدخول غير المشروع إلى النظام المعلوماتي، وكذلك سنتطرق الي التميز بين جريمة الدخول غير المشروع وما يرتبط بها وفقاً لما يلي:

المطلب الأول: مفهوم وفلسفة جريمة الدخول غير المشروع إلى النظام المعلوماتي.

المطلب الثاني: التميز بين جريمة الدخول غير المشروع وما يرتبط بها.

المطلب الأول: مفهوم وفلسفة جريمة الدخول غير المشروع إلى النظام المعلوماتي

تتناول هذه الدراسة بحث التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي، مما يجب معه البحث في مفهوم جريمة الدخول غير المشروع والمقصود بالنظام المعلوماتي، إلا أنه وجب علينا التعرض لتعريف الجرائم المعلوماتية كون أن جريمة الدخول غير المشروع هي أهم صورة من صور الجرائم المعلوماتية، وذلك لرسم الصورة العامة لذلك البناء البحثي، وصولاً لمفهوم وفلسفة جريمة الدخول غير المشروع إلى النظام المعلوماتي. وسوف نتطرق لذلك الأمر من خلال تقسيم ذلك المبحث إلى ثلاث فروع أساسية كما يلي:

الفرع الأول: تعريف جريمة الدخول غير المشروع.

الفرع الثاني: المقصود بالنظام المعلوماتي.

الفرع الثالث: فلسفة تجريم الدخول غير المشروع إلى النظام المعلوماتي.

[19] النوايسة، عبد الإله محمد سالم، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، ع 1، س 10، عام (2016)، ص (13-14).

الفرع الأول: تعريف جريمة الدخول غير المشروع

ونظراً لكون جريمة الدخول غير المشروع هي إحدى أهم صور الجرائم المعلوماتية فوجب التنويه في البداية إلى المقصود بالجرائم المعلوماتية لكي يتم رسم الصورة العامة لهذا البناء المعرفي، فمن المتفق عليه أنه لبحث أي فرع من الفروع يكون وجوباً علينا تعريف سماته الأساسية، ورغم أن الفقه الجنائي لم يتفق على إيراد تسمية موحدة للمقصود بالجرائم المعلوماتية (information crimes) فهناك من يطلق عليها تسمية الجرائم الإلكترونية، وهناك من يطلق عليها جرائم الإنترنت، إلا أن اختلاف تعريفهم لتلك الجرائم جاءت من اختلافهم إلى زاوية النظر لتلك الجريمة، إلا أنه نستخلص من كل ذلك التعريف الأمثل للجريمة المعلوماتية أو الإلكترونية حسب ما نراه تعريفاً جامعاً وافياً لوصف تلك الجرائم المعلوماتية.

أولاً: تعريف الجرائم المعلوماتية

عرف الفقهاء المقصود من الجرائم المعلوماتية بأنها: (سلوك غير مشروع، معاقب عليه قانوناً، صادراً عن إرادة جرمية، محله معطيات الكمبيوتر). [20]

وهذا التعريف يعتبر الأمثل لعدة أمور منها أنه كونه أحاط إحاطة شاملة بظاهرة جرائم تقنية المعلومات كما أنه عبر عن الطابع الفني المميز لتلك الجرائم ويتيح أيضاً إمكانية التعامل مع أي من التطورات التقنية المستقبلية، ومع جعل محل الجرائم المعلوماتية معطيات الكمبيوتر فقد تفرد هذا التعريف إلى الإشارة إلى إمكانية حصول الجرائم المعلوماتية عن طريق الامتناع وهو ما أغفلته بعض التعريفات الأخرى. [21]

وهذ التعريف هو ما تبناه نظام مكافحة جرائم المعلوماتية السعودي في مادته الأولى في الفقرة (8) حيث عرف الجريمة المعلوماتية بأنها "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام". وجاء أيضاً بالفقرة (3) من ذات المادة المقصود بالشبكة المعلوماتية حيث عُرفت بأنها "ارتباط بين أكثر من حاسب الآلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبمة العالمة (الإنترنت)". وأما عن تعريف المقصود بالحاسب الآلي فقد جاء بالفقرة (6) من ذات المادة بأن المقصود به هو "أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي

[20] د: حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في الجرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، القاهرة، عام (2004)، ص (1).
[21] د: البشري، محمد الأمين، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، عام (2000)، ص (6-7).

على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرنامج، والأوامر المعطاة له". [22]

ومن الملاحظ أن تعريف النظام السعودي كان مقتصراً على معيار الوسيلة التي ترتكب بها الجرائم المعلوماتية أكثر من محل الجريمة فاهتم بتعرف المقصود بالشبكة المعلوماتية والحاسب الآلي كوسيلة لارتكاب الجرائم المعلوماتية.

ثانياً: تعريف جريمة الدخول غير المشروع

سوف نتطرق لتعريف جريمة الدخول غير المشروع لغة وفقهاً ونظاماً من خلال الآتي:

تعريف جريمة الدخول غير المشروع في اللغة:

من أجل الوصول للتعريف اللغوي لجريمة الدخول غير المشروع في اللغة سنتناوله من خلال تعريف المقطع اللغوي المكون لها على النحو التالي:

الجريمة في اللغة: مفرد جمعها أجرام وجروم وجرائم، مصدر جرم والجيم والراء والميم أصل واحد يرجع إليه الفرع ويدل على الذنب ويقال: أجرم جرماً أي أذنب ذنباً. وعند أهل اللغة تعني الجناية أو الذنب جاء في لسان العرب: "وجرم إليهم وعليهم جريمة وأجرم جنى جناية". [23]

وقد وردت ألفاظ مجرم وجريمة وجرم في القرآن الكريم والسنة النبوية وفي شعر العرب في عدة مواضع منها الآتي:

في القرآن الكريم قال تعالى: ﴿إِنَّ الَّذِينَ أَجْرَمُوا كَانُوا مِنَ الَّذِينَ آمَنُوا يَضْحَكُونَ﴾[24].

وفي السنة، عن عامر بن سعد بن أبي وقاص عن أبيه أن النبي صلى الله عليه وسلم قال: (أعظم المسلمين جرمًا من سأل عن أمر لم يحرم فحرم على الناس من أجل مسألته)[25]

[22] المادة الأولى من نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/8 هـ الموافق 2007/3/27 م.
[23] أبن منظور، لسان العرب، دار أحياء التراث العربي، بيروت، عام (1419هـ)، (ج12 / 92) ص (97).
[24] سورة المطففين، الآية: 29.
[25] الحديث متفق عليه، رواه البخاري، باب ما يكره من كثرة السؤال حديث رقم(72893) الجامع الصحيح، دار الشعب، القاهرة ط1، 1407هـ 1987م.

وفي الشعر قال: "جرمت فزارة بعدها أن يغضبوا" ينسب البيت إلى أبي أسماء بن الضريبة، ومطلعه: ولقد طعنت أبا عيينة طعنة[26]

الدخول في اللغة: دخل يدخل دخولاً ومدخلاً، والدخول نقيض الخروج.[27]

وفي القرآن الكريم قال تعالى:﴿ وَقَالَ يَا بَنِيَّ لَا تَدْخُلُوا مِنْ بَابٍ وَاحِدٍ وَادْخُلُوا مِنْ أَبْوَابٍ مُتَفَرِّقَةٍ وَمَا أُغْنِي عَنْكُمْ مِنَ اللَّهِ مِنْ شَيْءٍ إِنِ الْحُكْمُ إِلَّا لِلَّهِ عَلَيْهِ تَوَكَّلْتُ وَعَلَيْهِ فَلْيَتَوَكَّلِ الْمُتَوَكِّلُونَ ﴾[28]

وجاء في الشعر الدخل ليس بالفصيح، وكذلك الدخل بالتحريك، يقال: هذا الأمر فيه دخل.[29]

غير المشروع في اللغة: المشروع عمل مسوغ أي ما سوغه الشرع ويأتي بمعنى الطرق المشروعة لكسب الشيء وبمعنى جائز. [30] وبالتالي يكون المقصود لغة بغير المشروع هو الممنوع أو غير المصرح به أو الغير مسوغ وهو بمثابة المحظور والمنهي عنه.

تعريف جريمة الدخول غير المشروع في الفقه الجنائي:

على الصعيد الفقهي يرى العديد من الفقهاء أن التشريعات التي لم تضع تعريفاً لجريمة الدخول غير المشروع هي الأكثر سلاسة ومسلكها هو الأفضل، لأن تجريم الدخول غير المشروع يرتبط ارتباطاً وثيقاً بأمور متغيرة ومتطورة كما بينا سابقاً، ومن ثم يرى العديد من الفقهاء أن وضع تعريف لجريمة الدخول غير المشروع قد يضيق من نطاق التجريم حال عجز التعريف عن مجاراة واستيعاب المستجدات التفننية التي تتطور بشكل مستمر وفعال. [31]

شمل التعريف الفقهي لجريمة الدخول غير المشروع العديد من التعريفات فيرى البعض بأنها "الولوج غير المصرح به أو بشكل غير مشروع إلى نظام معالجة البيانات باستخدام الحاسوب". [32]

---

[26] العامري، سليمان بن إبراهيم بن أمان، جريمة الدخول غير المشروع على المواقع الإلكترونية المتعلقة بأمن الدولة: دراسة تأصيلية تطبيقية في النظام السعودي، المجلة الأكاديمية للأبحاث والنشر العلمي، الإصدار الرابع والأربعون، تاريخ الإصدار 5-12-2022م، ص (333).

[27] الأزهري، تهذيب اللغة، الطبعة السابعة، ص (122).

[28] سورة يوسف، الآية: 67.

[29] الجوهري، إسماعيل بن حماء، معجم الوسيط، دار المعرفة بيروت، ط 6 (عام 1435هـ)، ص (335).

[30] معجم المعاني الجامع، مكتبة الشروق الدولية، المجلد 1، ص (210).

[31] النوايسة، عبد الإله محمد سالم، مرجع سابق، ص (33).

[32] د: القطري، محمد نصر محمد، الإشكاليات القانونية لحماية سلامة المعلومات: دراسة تطبيقية على الحماية الجنائية من الإتلاف المعلوماتي، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، مج 24، ع 93، إبريل 2015م. ص (171).

فحين يرى البعض الآخر بأنها "كافة الأفعال التي تسمح بالدخول إلى نظام معلوماتي ولإحاطة أو السيطرة على المعطيات التي يتكون منها أو الخدمات التي يقدمها". [33] كما عرفت أيضاً جريمة الدخول غير المشروع بأنها "ظاهرة معنوية تعني الدخول إلى العمليات التي يقوم بها النظام المعلوماتي". [34] وعلى الجانب الآخر أضاف بعض الفقهاء جانب مكاني للتعريف بمعنى التسلل إلى داخل النظام المعلوماتي، وجانب آخر زماني يتمثل في تجاوز حدود الفترة المصرح بالدخول خلالها. [35]

وقد اقترح الفقيه (Orin Kerry) من جامعة جورج واشنطن تعريفاً موسعاً لمفهوم الدخول غير المشروع لمسايرة التطور التكنولوجي حيث عرفه بأنه أي تفاعل ناجح مع الكمبيوتر (Any successful interaction with the computer) [36]

أما ما ذهب إليه البعض في تعريف جريمة الدخول غير المشروع أن جريمة الدخول تبدأ من اللحظة التي تم فيها تشغيل الحاسوب أو ما ذهب إليه آخرين من أنها تبدأ من خلال قدرة الفاعل على الاطلاع البصري أو السمعي على النظام المعلوماتي فلا يمكننا التسليم بتلك الآراء كون أن مجرد تشغيل الحاسوب لا يعني حدوث جريمة الدخول غير المشروع إذ أن جريمة الدخول غير المشروع تتطلب الولوج والانتقال إلى داخل النظام المعلوماتي، كما أنه قد يكون الحاسوب في وضع الحماية رغم تشغيله، كما أن اعتبار جريمة الدخول غير المشروع قد تحقق بمجرد أن يصبح الفاعل قادراً على الاطلاع السمعي أو البصري على النظام المعلوماتي فلا يمكننا التسليم به أيضاً، فقد ينتقل الفاعل إلى النظام بالفعل ولكنه يفشل بسب أو لأخر على الاطلاع على بيانات ومعلومات النظام المعلوماتي، فلكي تتحقق جريمة الدخول غير المشروع لابد من أن يحدث أتصال فعلي من قبل الجاني بمعلومات وبيانات النظام المعلوماتي، فلا يكفي محاولة إقامة الاتصال فالجاني غالبا يجري العديد من محاولات الاتصال بالنظام المعلوماتي حال تخمينه كلمة السر على سبيل المثال، فبالتي لا تتحقق جريمة الدخول غير المشروع للنظام المعلوماتي إلا بعد الحصول على كلمة السر والتمكن من التسلل والسيطرة على النظام المعلوماتي والاطلاع على كافة البيانات والمعلومات

[33] العبيدي، أسامة غانم، جريمة الدخول غير المشروع إلى النظام المعلوماتي: دراسة قانونية في ضوء القوانين المقارنة، مجلة دراسات المعلومات، ع 14، مايو 2012م. ص (13).

[34] بوزيدي، مختارية، ماهية الجريمة الإلكترونية، بحث مقدم في الملتقي الوطني: أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر،2017/3/29م، ص (14).

[35] ناصر، حمودي، الحماية الجنائية للتجارة الإلكترونية، رسالة ماجستير، جامعة الجزائر، عام 2015م.، ص (83).

[36] Orin S. Kerr: Cybercrime's Scope: Interpreting (Access) and Authorization NYU Law Review, Vol. 78, No. 5, pp. 1596-1668, November 2003, p..1620

أو الخدمات التي يقدمها النظام المعلوماتي[37]. وهو ما سنوضحه ونبينه بمزيد من البحث في الحديث عن أركان جريمة الدخول غير المشروع إلى النظام المعلوماتي.

تعريف جريمة الدخول غير المشروع نظامياً:

من خلال البحث في التشريعات التي عالجت ونصت على جريمة الدخول غير المشروع إلى النظام المعلوماتي، نجد أنها اختلفت مع بعضها البعض في العديد من الأمور ومن أولها مسمى جريمة الدخول غير المشروع ذاتها فالمشرع السعودي في نظام مكافحة جرائم المعلوماتية، وكذلك المشرع المصري في قانون مكافحة جرائم مكافحة تقنية المعلومات رقم 175 لسنة 2018، والمشرع الكويتي في القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات، قد توافقوا على تسميتها جريمة الدخول غير المشروع، وهناك تشريعات أطلقت عليها جريمة الدخول دون تصريح ومنها المشرع الأردني في قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023، وأما المشرع العماني فقد أطلق عليها الدخول بدون وجه حق في المرسوم السلطاني رقم 12/ 2011 كما وافقه في ذلك المشرع القطري في القانون رقم 14 لسنة 2014 بشأن قانون مكافحة الجرائم الإلكترونية، وأما المشرع البحريني في القانون رقم 60 لسنة 2014 بشأن جرائم تقنية المعلومات فقد أطلق عليها جريمة الدخول دون مسوغ قانوني. أما المشرع الإماراتي في المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية أطلق عليها في مادته الثانية الاختراق الإلكتروني وعرف المشرع الاماراتي المقصود بالاختراق في مادته الأولى في التعريفات بأنه الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب الآلي وما في حكمها.

وأما عن القوانين الأجنبية فمصطلح (Unauthorized Access) هو المصطلح الشائع في العديد التشريعات الأجنبية التي تعاقب على جريمة الدخول غير المشروع[38]. كما يطلق أيضاً مصطلح جريمة

[37] د: نصر أحمد، شريف، الجوانب الموضوعية لجرائم الدخول غير المشروع إلى الأنظمة المعلوماتية: دراسة مقارنة، مجلة كلية الشريعة والقانون بطنطا، العدد الخامس والثلاثون، يونيو 2020م.، ص (922).

[38] انظر على سبيل المثال المادة 2 من قانون إساءة استخدام الكمبيوتر الإنجليزي لسنة 1990، المادة 615 من قانون العقوبات الإيطالي، المادة 550 من قانون العقوبات البلجيكي.

الدخول غير القانوني (illegal Access) عند البعض الآخر [39] وهناك من التشريعات التي أطلقت عليها جريمة الدخول إلى النظام المعلوماتي بطريق الغش والخداع كالمشرع الفرنسي. [40]

وأن كنا نميل إلى تأييد الرأي الفقهي الذي يرى أن التشريعات والنظم القانونية التي لم تضع تعريفاً لجريمة الدخول غير المشروع هي الأكثر سلاسة ومسلكها هو الأفضل، لأن تجريم الدخول غير المشروع يرتبط ارتباطاً وثيقاً بأمور متغيرة ومتطورة كما بينا سابقاً، إلا أنه العديد من التشريعات والنظم القانونية أفردت في طيات تشريعاتها تعريفاً لجريمة الدخول غير المشروع وكما أختلف الفقهاء في تعريف جريمة الدخول غير المشروع واختلفت التشريعات الدولية في مسمى الجريمة ذاتها كما اختلفوا أيضاً في التعريف النظامي والتشريعي لجريمة الدخول غير المشروع في على سبيل المثال:

في نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم (م/ 17) بتاريخ 1428/3/8 هـ الموافق 2007/3/27 م. جاء في مادته الأولى من الفقرة السابعة تعريف الدخول غير المشروع بأنه "دخول شخص بطريقة متعمدة إلى حاسب الآلي، أو موقع، إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها".

أما في قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 في مادته الأولى عرف الاختراق بأنه "الدخول غير المصرح به أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة إلى نظام معلوماتي أو حاسب آلي أو شبكة معلوماتية وما في حكمها.

وكذلك نهج المشرع الإماراتي ذات النهج فعرف في مادته الأولى في التعريفات الخاصة بالمرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية الاختراق بأنه "الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها". وكذلك عرف قانون مكافحة جرائم تقنية المعلومات الكويتي رقم 63 لسنة 2015م. في مادته الأولى أيضاً الدخول غير المشروع بأنه "النفاذ المتعمد غير المشروع لأجهزة الحاسب الآلي، أو لنظام معلوماتي أو شبكة معلوماتية، أو موقع الكتروني من خلال اختراق وسائل وإجراءات الحماية أو بالتجاوز للتفويض الممنوح".

[39] انظر على سبيل المثال المادة 145 من قانون العقوبات النرويجي، المادة 263 من قانون العقوبات الدنماركي.
[40] انظر على سبيل المثال المادة 323 / 1 من قانون العقوبات الفرنسي.

ومن خلال النظرة الدقيقة والبحث في جل التشريعات العربية والأجنبية التي عرفت جريمة الدخول غير المشروع نجد أن المشرع السعودي لم يشترط لقيام الجريمة أن يكون النظام المعلوماتي أو الحاسب الآلي، أو موقع، إلكتروني محمي بحظر الدخول عليه مثلما انتهجت العديد من التشريعات كالمشرع الكويتي وغيره. فالمشرع السعودي لم يشترط أن يكون النظام محمياً بكلمة سر مثلاً، بل اعتبر الدخول غير المشروع معاقب عليه حتى ولو لم يعني صاحبه أن يحميه من تطفل الآخرين ولكن نجد أن المشرع اشترط أن يكون الدخول غير المشروع كان بقصد تحقيق غاية معينة وتوافرت به نية معينة وهو ما يعرف بالقصد الجنائي الخاص.

وأما عن التشريعات الأجنبية فقد تباينت أيضاً في وجوب توفر الحماية من عدمه للنظام المعلوماتي، فمنهم من اشترط الحماية للمواقع أو الأنظمة المعلوماتية حتى تشملها الحماية الجنائية ومنهم من شمل كافة الأنظمة المعلوماتية بالحماية الجنائية دون اشتراط أن تكون تلك الأنظمة محمية، ومن هذه التشريعات التي اشترط الحماية نجد قانون العقوبات الإيطالي، المكسيكي، الفنلندي، اليوناني، الألماني، السويسري [41] أما القانون الأمريكي الفيدرالي اشترط أن يتم الدخول غير المصرح به إلى حاسب الآلي محمي على وجه الحصر في مؤسسة مالية أو حكومية فيدرالية أو بين ولايتين أو بالتجارة الأجنبية أو بالاتصالات [42] أما المشرع الفرنسي لم يشترط أن يكون النظام المعلوماتي محمي بأحد صور الحماية، بل جعل التجريم يشمل كافة النظم المعلوماتية والمواقع المحمية والغير محمية. [43]

إن جل ملاحظاتنا على تعريف المشرع السعودي للدخول غير المشروع تكمن في ملاحظتان الملاحظة الأولى هو أن المشرع قد اقتصر في التعريف على حالة الجاني التي لا يتمتع بتصريح للدخول، وهو ما يعني فتح المجال لإباحة باقي الطرق والحالات على سبيل المثال حالة تجاوز شروط الترخيص، أو البقاء بشكل غير مشروع عند وجود تصريح سابق، وهو ما نجد أن المشرع المصري قد تلاشى تلك الملاحظة في التعريف السابق.

[41] أنظر المادة 615 من قانون العقوبات الإيطالي، المادة 211 من قانون العقوبات المكسيكي، المادة 38 من قانون العقوبات الفنلندي، المادة 370 من قانون العقوبات اليوناني، المادة 202 من قانون العقوبات الألماني، المادة 143 من قانون العقوبات السويسري.

[42] Dr: Rizgar Kadir, International Solution, 27Tex.Int. L.J. (l992). P496- 497, Shackelford. S: Computer- Related Sharia & Law, IssueNo.40-October 2009, p. 56.

[43] د: عطا الله، شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق عام2005، ص (118).

والملاحظة الثانية هو أن المشرع السعودي قد اقتصر على حالة الدخول العمدي وبالتالي أباح الدخول غير العمدي عن طريق الخطأ وهو ما تلاشاه أيضاً المشرع المصري على سبيل المثال في المادة (14) من القانون رقم 175 لسنة 2018 حيث تعرض إلى حالة الدخول العمدي وكذلك حالة الدخول بخطأ غير عمدي والبقاء بدون وجه حق.

الفرع الثاني: المقصود بالنظام المعلوماتي

أن أهمية الوصول للمقصود بالنظام المعلوماتي تكمن في أنه محل الجريمة الإلكترونية عموماً، وجريمة الدخول غير المشروع خصوصاً. لذا سوف نتطرق للمقصود بالنظام المعلوماتي لغة وفقهاً ونظاماً من خلال الآتي:

أولاً: المقصود بالنظام المعلوماتي في اللغة:

من أجل الوصول للتعريف اللغوي للمقصود بالنظام المعلوماتي في اللغة سنتناوله من خلال تعريف المقطع اللغوي المكون لها على النحو التالي:

النظام في اللغة: مفرد جمعها نُظُم وأنظمة وأناظيم، ويقصد به الترتيب والاتساق. ونظمت الأمر فانتظم، أي أقمته فاستقام. والنظام بكسر النون وتشديدها العقد من الجوهر والخرز ونحوها، ويقال ليس لأمرهم نظام أي ليس له هدي ولا متعلق ولا استقامة [44] وجاء في المعجم الوسيط نظام الأمر: قوامه وعماده.[45]
المعلومات في اللغة: المعلومات في اللغة جمع لكلمة معلومة وأصلها مشتقة من كلمة علم بفتح العين وكسر اللام، والعلم نقيض الجهل، ويقال رجل عالم وعليم، ويقصد به الإدراك والوعي والإحاطة ببواطن الأمور. [46]

وفي القرآن الكريم قال تعالى: ﴿ الْحَجُّ أَشْهُرٌ مَّعْلُومَاتٌ فَمَن فَرَضَ فِيهِنَّ الْحَجَّ فَلاَ رَفَثَ وَلاَ فُسُوقَ وَلاَ جِدَالَ فِي الْحَجِّ وَمَا تَفْعَلُواْ مِنْ خَيْرٍ يَعْلَمْهُ اللّهُ وَتَزَوَّدُواْ فَإِنَّ خَيْرَ الزَّادِ التَّقْوَى وَاتَّقُونِ يَا أُوْلِي الأَلْبَابِ﴾[47]

[44] أبن منظور، محمد بن مكرم، لسان العرب، عام (1993م)، ج12، ص (197).
[45] المعجم الوسيط، الصادر عن مجمع اللغة العربية، بمصر، ط 1381هـ، 1961 م، ج2، ص (841).
[46] أبن منظور، محمد بن مكرم، لسان العرب، عام (1993م)، ج12، ص (417).
[47] سورة البقرة. الآية: 197

ثانياً: المقصود بالنظام المعلوماتي في الفقه الجنائي:

على الصعيد الفقهي تختلف الآراء والتعريفات حول المقصود بالنظام المعلوماتي فهذا المصطلح يعد من أكثر المصطلحات إثارة للجدل في وقتنا الحالي وتكمن أهمية بيان المقصود بالنظام المعلوماتي كونه محل جريمة الدخول غير المشروع وبالتالي فإن التعريف الدقيق للمقصود بالنظام المعلوماتي يمكن المشرع الجزائي من الإحاطة بكافة جوانب الحماية المختلفة التي يحتاجها النظام المعلوماتي حتى يتمكن المشرع الجزائي من سبغ حمايته الفعالة عليه.

من الملاحظ أنه يصعب تحديد مفهوم شامل للمقصود بالنظام المعلوماتي الذي يحاول المشرع الجزائي حمايته في نظام مكافحة جرائم المعلوماتية كون هناك تباين كبير جداً في تحديد المقصود بالنظام المعلوماتي وذلك لصعوبة مواكبة أشكال المعلومات التي تظهر باستمرار بأشكال جديدة وذلك لكونها مرتبطة ارتباطاً وثيقاً بتكنولوجيا الحاسوب والشبكات والإنترنت مما يصعب تحديد مفهومها ووضعها في إطار محدد ودقيق مما دفع بعض الفقهاء والباحثين إلى القول باستحالة تحديد مفهوم المعلومات أو وصف دقيق لها، ولكن يمكن إدراك آثارها فقط. [48]

ورغم ذلك عرف بعض علماء التقنية المقصود بالنظام المعلوماتي "بأنه النظام الذي يتضمن مجموعة متجانسة ومترابطة من الأعمال والموارد تقوم بتجميع وتشغيل وإدارة البيانات بغرض إنتاج وتوصيل معلومات مفيدة لمستخدمي القرارات من خلال شبكة القنوات وخطوط الاتصال".[49]

ثالثاً: المقصود بالنظام المعلوماتي نظامياً:

من خلال البحث في التشريعات العربية التي عالجت ونصت على تعريف المقصود بالنظام المعلوماتي، نجد أنها متشابهة إلى قدر كبير في تحديد المقصود بالنظام المعلوماتي بما جاء به المشرع السعودي في نظام مكافحة جرائم المعلوماتية الذي صدر بقرار رئيس مجلس الوزراء رقم 79 بتاريخ 1428/3/7 هـ. وصدق عليه بالمرسوم الملكي رقم (م/17) بتاريخ 1428/3/8هـ. الموافق 2007/3/27 م.، قد عرف المقصود بالنظام المعلوماتي في مادته الأولى في الفقرة الثانية بأنه "مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الألية".

[48] المناصير، حسن فضيل خليف، وربيع، عماد محمد أحمد، جريمة الدخول غير المشروع إلى النظام المعلوماتي والتعدي على محتوياته: دراسة مقارنة، رسالة ماجستير، جامعة جريش، الأردن، عام 2016م، ص (17).
[49] حسين، أحمد حسين، وربيع، نظم المعلومات المحاسبية، الإطار الفكري والنظم التطبيقية، مكتبة الإشعاع الفنية، القاهرة، 1998م، ص (21).

وكذلك سايره المشرع المصري في قانون مكافحة جرائم مكافحة تقنية المعلومات رقم 175 لسنة 2018 م، حيث عرف المقصود بالنظام المعلوماتي في مادته الأولى بأنه "مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية".

وقد نهج المشرع القطري ذات النهج في القانون رقم 14 لسنة 2014 بشأن قانون مكافحة الجرائم الإلكترونية في بابه الأول وفي مادته الأولى عرف المقصود بالنظام المعلوماتي بأنه "مجموعة برامج وأجهزة، تستخدم لإنشاء أو استخراج المعلومات، أو إرسالها، أو استلامها، أو عرضها، أو معالجتها، أو تخزينها".

وكذلك المشرع العماني فقد عرف النظام المعلوماتي في المرسوم السلطاني رقم 12/ 2011 بشأن إصدار قانون مكافحة جرائم تقنية المعلومات وذلك في المادة الأولى من الفصل الأول في الفقرة (ى) حيث عرف النظام المعلوماتي بأنه "مجموعة برامج وأدوات تستخدم في معالجة وإدارة البيانات والمعلومات الإلكترونية".

وعن المشرع الأردني قد انتهج ذات النهج في قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023، وعرف نظام المعلومات في مادته الثانية بأنه "مجموعة البرامج أو التطبيقات أو منصات التواصل الاجتماعي أو الأجهزة أو الأدوات المعدة لإنشاء البيانات أو المعلومات إلكترونياً، أو إرسالها أو تسلمها أو معالجتها أو تخزينها أو إدارتها أو عرضها بالوسائل الإلكترونية".

وأما المشرع الكويتي فقد اختلف في تسمية النظام المعلوماتي وأطلق عليه مسمى نظام الحاسب الآلي وعرفه القانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات في مادته الأولى من الفصل الأول بأنه "مجموعة برامج وأنظمة معلوماتية معدة لتحليل المعلومات والبيانات والأوامر وبرمجتها وإظهارها أو حفظها أو إرسالها أو استلامها، ويمكن أن تعمل بشكل مستقل أو بالاتصال مع أجهزة أو أنظمة معلوماتية أخرى".

أما عن المشرع الإماراتي فقد توسع في مفهوم النظام المعلوماتي في المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية عرف المقصود بنظام المعلومات الإلكتروني في مادته الأولى بأنه "برنامج معلوماتي أو مجموعة البرامج المعلوماتية المعدة لمعالجة أو إدارة أو تخزين المعلومات الإلكترونية القابلة لتنفيذ التعليمات أو الأوامر بوسائل تقنية المعلومات، ويشمل التطبيقات أو ما في حكمها".

من خلال التعريفات السابقة يتبين أنه لا يوجد أي اختلافات جوهرية في تعريف المقصود بالنظام المعلوماتي في التشريعات العربية حيث اعتمدت جل التشريعات في مفهوم النظام المعلوماتي على الوظيفة الأساسية التي تقوم مجموعة البرامج والأدوات من معالجة البيانات والمعلومات أو تحليلها أو إدارتها أو استخراجها أو برمجتها أو أنشائها أو ارسالها أو استقبالها أو تصفحها أو تخزينها وحفظها أو عرضها أو تقديم خدمة معلوماتية من خلالها.

وهذه الوظائف ذكرها المشرع السعودي في نظام مكافحة جرائم المعلوماتية حين عرف المقصود بالحاسب الآلي في مادته الأولى بالفقرة السادسة حيث عرف الحاسب الآلي بأنه "أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له".

الفرع الثالث: فلسفة تجريم الدخول غير المشروع إلى النظام المعلوماتي

تكمن فلسفة المشرع في تجريم الدخول غير المشروع إلى النظام المعلوماتي في أن هذه الجريمة تمثل تهديداً لمستودع السر المعلوماتي الرقمي، كما أنها تعد انتهاكاً صارخاً للخصوصية الإلكترونية حيث تهدد جريمة الدخول غير المشروع العديد من المصالح المحمية سوء محمية من الحكومة أو الأفراد أو المؤسسات، حيث أغلب الحكومات في العصر الحالي تعتمد على الأنظمة المعلوماتية مما قد يهدد أمن الدولة واقتصادها. كما تحتوي الأنظمة المعلوماتية للأفراد على معلومات تتصل بالحياة الخاصة بهم مما يشكل الوصول إليها عن طريق الدخول غير المشروع انتهاكا للحق في الخصوصية. كما أنه على مستوى المؤسسات التجارية والاقتصادية تشكل جريمة الدخول غير المشروع خطراً على مصالحها وأموالها من خلال الاطلاع على أسرارها التجارية أو الاعتداء على حقوق ملكيتها الفكرية، مما يزعزع الثقة في المعاملات التجارية الإلكترونية.

وقد أشارت اللجنة القانونية في البرلمان الإنجليزي إلى العديد من أسباب وفلسفة تجريم الدخول غير المشروع للنظام المعلوماتي في قانون إساءة استخدام الكمبيوتر لسنة 1990م. وكان من أهم تلك الأسباب لتجريم الدخول غير المصرح به المجرد (Mere Access) هو الخسائر التي يتم تكبدها والتكاليف التي يتحملها مالكي أنظمة الحواسيب التي يتم اختراق أنظمتها الأمنية وكذلك أن جريمة الدخول غير المشروع إلى النظام المعلوماتي قد يكون تمهيد ومرحلة لارتكاب سلسلة من الجرائم الأخرى وأيضاً تخفيض الاستثمارات العامة في أنظمة الحاسوب.

ولأهمية تجريم جريمة الدخول غير المشروع إلى النظام المعلوماتي نجد أن تلك الجريمة تتصدر التشريعات التي عنيت بمكافحة الجرائم المعلوماتية وتنص عليها كافة التشريعات بغض النظر عن أساليب التجريم وفلسفة العقوبات المتبعة، علاوة على كما أوضحنا سالفاً بأن أغلب الجرائم المعلوماتية يستلزم ارتكابها المرور بجريمة الدخول غير المشروع، لذا يطلق أغلب الباحثون على جريمة الدخول غير المشروع إلى النظام المعلوماتي أنها أم الجرائم الإلكترونية.

فالدخول غير المشروع إلى النظام المعلوماتي قد يهدد أسرار الدول والشركات وكذلك الأفراد، مما يرتب مجرد الاطلاع عليها أو الحصول عليها خسائر مالية أو معنوية فادحة لا يمكن تعويضها.

وتكمن فلسفة المشرع أيضاً في تجريم الدخول غير المشروع إلى النظام المعلوماتي بجانب خطورة الجريمة كما بينا سالفة في أن أفعال الدخول غير المشروع إلى النظام المعلوماتي والاختراقات قد انتشرت بصورة واسعة بسب تزايد التطور التكنولوجي الملحوظ في عصرنا الحالي وعدم اهتمام كثير من الأفراد، والشركات، وكذلك بعض مؤسسات الدول بتوفير الأمن والحماية التقنية للأنظمة المعلوماتية التي يتعاملون بها، وعلى الجانب الآخر فقد أصبحت برامج الاختراق وأساليبه وأدواته متاحة عبر الإنترنت مما أدى إلى زيادة هائلة في عدد من يرتكبون تلك الجريمة.

كما أن من أهم أسباب المشرع في فلسفته في التجريم بجانب خطورة الجريمة في أن البيانات والمعلومات تكون ضعيفة داخل النظام المعلوماتي بحيث يمكن الاعتداء عليها بسهولة وتتميز أيضاً بالضخامة والتنوع والأهمية في ذات الوقت لذا دعت الحاجة التشريعية إلى توفير الحماية الجزائية للنظام المعلوماتي من الدخول غير المشروع له.

وعلى الرغم من وضوح علة المشرع في فلسفته لتجريم الدخول غير المشروع للنظام المعلوماتي إلا أنه اتجه بعض الفقهاء إلى أنه لا جدوى حقيقية أو ضرورية لهذا التجريم، ويرون أن الدخول إلى النظام المعلوماتي ولو بدون وجه حق هو مجرد استعراض لقدرات المتطفل على النظام المعلوماتي وخاصة في الحالات التي لا تترك أثراً يدل عليها أو التي لا تحدث بسببها أضرار ملحوظة على البيانات أو المعلومات، وكذلك يبررون بصعوبة جهات التحقيق من إثبات الدخول غير المشروع إلى النظام المعلوماتي.[50]

[50] راجع في عرض مبررات هذا الاتجاه: أ/ عباوي، نجاة، الإشكاليات القانونية في تجريم الاعتداء على أنظمة المعلومات، مجلة دراسات المعلومات، ع 14، مايو2012م، ص (12).

بيد أن أغلب الفقهاء والباحثين في مجال الجرائم المعلوماتية يرفضون هذا الرأي، وينادون بضرورة تجريم الدخول غير المشروع إلى النظام المعلوماتي كونها مدخلاً أساسياً لارتكاب الكثير من الجرائم المعلوماتية الأخرى وتمثل أيضاً تلك الجريمة تهديداً حقيقياً وخطيراً على مستودع السر الإلكتروني.[51]

أن من أهم فلسفة التجريم للدخول غير المشروع إلى النظام المعلوماتي تكمن في أن تجريم الدخول غير المشروع إلى النظام المعلوماتي له أهمية فائقة تظهر في تلك الحالات في الجرائم المعلوماتية التي لا ينطبق على وقائعها نص تجريمي محدد، إذ يمكن أن ينطبق عليها وصف الدخول غير المشروع كون جل الجرائم المعلوماتية تستلزم المرور بجريمة الدخول غير المشروع.

المطلب الثاني: التميز بين جريمة الدخول غير المشروع وما يرتبط بها

هناك العديد من الجرائم التي ترتبط بجريمة الدخول غير المشروع إلى النظام المعلوماتي ارتباطاً وثيقاً وقد تعتبر في بعض الأحيان صورة من صور تلك الجريمة مما أوجب علينا التطرق إلى تلك الجرائم لبيان المقصود بها وتوضيح أهم ما يميزها عن جريمة الدخول غير المشروع النظام المعلوماتي، ومن أهم تلك الجرائم جريمة تجاوز حدود التصريح في النظام المعلوماتي. وكذلك جريمة البقاء غير المصرح به في النظام المعلوماتي. وأيضاً جريمة التنصت أو الالتقاط للبيانات في الشبكة المعلوماتية.

وسوف نتطرق لذلك الأمر من خلال تقسيم ذلك المطلب إلى ثلاثة فروع أساسية وهما كما يلي:

الفرع الأول: جريمة تجاوز حدود التصريح في النظام المعلوماتي.

الفرع الثاني: جريمة البقاء غير المصرح به في النظام المعلوماتي.

الفرع الثالث: جريمة التنصت أو الالتقاط للمعلومات في النظام المعلوماتي.

الفرع الأول: جريمة تجاوز حدود التصريح في النظام المعلوماتي

في الحقيقة الأمر حالة عدم وجود تصريح لدى الشخص للدخول إلى النظام المعلوماتي لا تثير ابتداءً أي إشكالاً كون أن في هذه الحالة نكون أمام جريمة الدخول غير المشروع في حالة اكتمال أركانها وشروطها، أما ما

[51] د/ الرواشدة، سامي، ود/ الهياجنة، أحمد، مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، المجلة الأردنية في القانون والعلوم والسياسة، مج 1، ع3، عام 2009م، ص (166).

تثيره حالة وجود هذا التصريح لدى الشخص فأننا نكون أمام شخص مصرح له بالدخول إلى النظام المعلوماتي وبالتالي فإن دخوله إلى النظام المعلوماتي لا يعد دخولاً غير مشروع.

إلا أنه تكون الإشكالية في حالة قيام الشخص بتجاوز حدود التصريح الممنوح له وذلك على اعتبار أن هذا التصريح يمتد إلى أجزاء معينة داخل النظام المعلوماتي دون غيرها ففي هذه الحالة عندما يتجاوز الشخص حدود ذلك التصريح نكون أمام جريمة تجاوز حدود التصريح في النظام المعلوماتي وغالباً ما يكون ذلك الشخص من العاملين لدى الجهة التي تم الدخول إلى نظامها المعلوماتي كونه يحوز تصريح بالدخول إليه.

وعلى الرغم من صعوبة معرفة إذا ما تجاوز الشخص حدود تصريحه الممنوح له من عدمه، وأيضاً إذا كان هذا التجاوز قد تم بصورة عدمية أو غير متعمد إلا أنه إذا ثبت بعد البحث أن الشخص قد تجاوز بصورة عمدية حدود التصريح الممنوح له إلى النظام المعلوماتي فإننا نكون بصدد ارتكاب جريمة تجاوز حدود التصريح في النظام المعلوماتي وليست جريمة الدخول غير المشروع إلى النظام المعلوماتي.

ومن هنا يكون قد اتضح جلياً الفرق الجوهري بين جريمة الدخول غير المشروع إلى النظام المعلوماتي وجريمة تجاوز حدود التصريح في النظام المعلوماتي كون جريمة تجاوز حدود التصريح في النظام المعلوماتي تحتاج إلى وجود تصريح مسبق لمرتكب الجريمة وتتطلب أيضاً أن يكون تجاوز تلك الحدود قد تم بشكل متعمد[52].

ومن خلال البحث بالتشريعات العربية نجد أن العديد من التشريعات قد تناولت جريمة تجاوز حدود التصريح إلى جانب جريمة الدخول غير المشروع ومن تلك التشريعات ما انتهجه المشرع الإماراتي في مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية حين عرف الاختراق بأنه "الدخول غير المرخص به أو المخالف لأحكام الترخيص أو الدخول بطريقة غير مشروعة أو البقاء بصورة غير مشروعة في نظام معلوماتي أو حاسب آلي أو نظام تشغيل جهاز أو آلة أو مركبة أو شبكة معلوماتية وما في حكمها". وعاقب عليهما جميعاً وفق المادة (2) ضمن الجرائم الواقعة على تقنية المعلومات.

أما المشرع الأردني في قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023، فقد عرف المقصود بالتصريح في مادته الثانية بأنه "الإذن الممنوح من صاحب العلاقة إلى شخص أو أكثر أو للجمهور للدخول أو الوصول إلى نظام المعلومات أو تقنية المعلومات أو الشبكة المعلوماتية أو استخدامها"، وفي مادته الثالثة في الفقرة

[52] خليفة، محمد مسعود محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، رسالة مقدمة للحصول على درجة الماجستير في الحقوق، كلية الحقوق، جامعة الإسكندرية، عام 2005-2006، ص (148).

الأولى نص على أنه "يعاقب كل من دخل أو وصل قصدًا إلى الشبكة المعلوماتية أو نظام المعلومات أو وسيلة تقنية المعلومات أو أي جزء منها بأي وسيلة دون تصريح أو بما يخالف أو يجاوز التصريح ...".

وكذلك نهج ذات النهج المشرع القطري في القانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية في مادته الثالثة في الفقرة الأولى حيث نص على "يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (500,000) خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من دخل عمداً، دون وجه حق، بأي وسيلة، موقعاً إلكترونياً، أو نظاماً معلوماتياً، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك....".

وأما المشرع العماني في المرسوم السلطاني رقم 12/ 2011 بإصدار قانون مكافحة جرائم تقنية المعلومات لم يخالف ذات النهج الذي انتهجته معظم التشريعات العربية ففي مادته الثالثة نص على "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على ستة أشهر وبغرامة لا تقل عن مائة ريال عماني ولا تزيد على خمسمائة ريال عماني أو بإحدى هاتين العقوبتين، كل من دخل عمداً ودون وجه حق موقعاً إلكترونياً أو نظاماً معلوماتياً أو وسائل تقنية المعلومات أو جزءً منها أو تجاوز الدخول المصرح به إليها أو استمر فيها بعد علمه بذلك...".

وأما المشرع الكويتي في القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات عندما عرف مفهوم الدخول غير المشروع لم يفرق بين جريمة تجاوز حدود التصريح في النظام المعلوماتي وجريمة الدخول غير المشروع بل جعل جريمة تجاوز حدود التصريح في النظام المعلوماتي صورة من صور الدخول غير المشروع ففي مادته الأولى عرف المشرع الكويتي الدخول غير المشروع بأنه "النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح".

ومن التشريعات العربية الأخرى التي تناولت جريمة تجاوز حدود التصريح في النظام المعلوماتي نجد أن المشرع المصري في القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات.

قد تميز عن باقي التشريعات العربية حيث أفرد مادة مستقلة بجريمة تجاوز حدود التصريح في النظام المعلوماتي وجعلها جريمة مستقلة عن جريمة الدخول غير المشروع حيث نصت المادة (15) من قانون مكافحة جرائم تقنية المعلومات على أنه "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن

ثلاثين ألف جنية ولا تتجاوز خمسين ألف جنية، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول".

وبالرجوع إلى المشرع السعودي في نظام مكافحة جرائم المعلوماتية، كما بينا سابقاً نجد أن المشرع السعودي اقتصر في التعريف الخاص بالدخول غير المشروع على حالة الجاني التي لا يتمتع بتصريح للدخول، وهو ما يعني فتح المجال لإباحة الطرق الأخرى مثل تجاوز شروط الترخيص وحدود التصريح الخاص بالدخول إلى النظام المعلوماتي، أو البقاء بشكل غير مشروع عند وجود تصريح سابق، إلا أنه بالتمعن في نظام مكافحة جرائم المعلوماتية السعودي نجد أنه نص في المادة الثامنة من النظام في فقرته الثانية على أنه "لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الأتية:

2. شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه".

وإن كنا نرى أن تلك المادة قد تحوي في طياتها بصورة أو بأخرى اتجاه المشرع السعودي إلى تجريم صورة من صور تجاوز حدود التصريح في النظام المعلوماتي في حالة قيام الموظف العام مستغلاً سلطته أو نفوذه من خلال ارتكاب جريمة الدخول غير المشروع إلى النظام المعلوماتي الخاص بوظيفته فمن المفترض أن يكون لذلك الموظف العام لديه تصريح بالدخول إلى النظام المعلوماتي الخاص بوظيفته وإلا كيف سيقوم باستغلال نفوذه وسلطته الوظيفية، إلا اننا ننتقد ما انتهجه المشرع السعودي من عدم النص صراحة على تجريم جريمة تجاوز حدود التصريح في النظام المعلوماتي أو البقاء غير المصرح به في النظام المعلوماتي مثلما انتهجته جل التشريعات العربية والعديد من التشريعات الاجنبية لما تمثله تلك الجريمة من خطورة على الأمن المعلوماتي.

وأما على صعيد التشريعات الأجنبية فنجد تباين بينهم فهناك من التشريعات التي نصت في تشريعاتها على جريمة تجاوز حدود التصريح في النظام المعلوماتي ومنها ما ذكره قانون العقوبات البلجيكي في المادة 550/ ب/ 2 حيث نص على تجريم تجاوز حدود وسلطة أي شخص بالدخول لنظام الحاسب الآلي(Exceeds his power of access to a computer system)، ومنها من وضع لها شروط خاصة مثلما نص عليه القانون اليوناني حيث أعتبر القانون اليوناني أن تجاوز حدود التصريح في النظام المعلوماتي عند دخول العاملين في المؤسسة الخاصة بالنظام المعلوماتي الخاص بهم لا يشكل جريمة، إلا إذا كان الدخول إلى النظام

المعلوماتي ممنوع صراحة بموجب الأنظمة الداخلية للمؤسسة أو بموجب قرار مكتوب من قبل الجائز الشرعي للنظام المعلوماتي أو من الموظف الذي ينوب عنه، وأما المشرع النيوزلندي في المادة 252 / 1 من قانون العقوبات بعدما جرم حالة الدخول غير المصرح به لنظام الحاسب الآلي، استثنت في فقرتها الثانية من ذات المادة تجريم حالة الدخول الشخص المصرح له بالدخول إلى نظام الحاسب الآلي ولو لغرض أخر غير الذي سمح له بالدخول من أجله وعلل ذلك لكونه تجنباً للشك في ارتكاب الجريمة من عدمه، وأما القانون الأمريكي لسنة 1986 بشأن الاحتيال وإساءة استخدام الحاسب الآلي فقد عرف تجاوز حدود التصريح في النظام المعلوماتي بأن "تجاوز الدخول المصرح به يكون في الحالة التي يتم فيها الدخول إلى الحاسب الآلي بتصريح واستخدام الدخول في الحصول على المعلومات أو تعديل المعلومات الموجودة بالحاسب الآلي التي لا يكون الشخص الذي دخل مخولاً في الحصول عليها أو تعديلها". [53]

وأما المشرع الإنجليزي ورغم قيامه بتجريم الدخول غير المشروع في قانون إساءة استخدام الحاسب الآلي إلا أن القضاء الإنجليزي قد تعرض إلى حالة تجاوز حدود التصريح المخول للشخص المصرح له للدخول إلى النظام المعلوماتي باعتبارها صورة من صور الدخول غير المشروع ففي حكم لموضوع قيام الأشخاص المصرح لهم بالدخول بأفعال خارج نطاق التصريح، أو ما يسمى الدخول المصرح به لغرض غير مصرح به (Authorized access fora unauthorized purpose)، ففي قضية Bignell [54]، والتي تتلخص وقائعها بقيام ضابطي شرط بالدخول إلى جهاز الحاسب الآلي التابع للإدارة التي يعملان بها للحصول على معلومات عن مركبات لأغراض خاصة، وتم إدانتهما من محكمة أول درجة بجرم الدخول غير المصرح به سندًا لأحكام المادة الأولى من قانون استخدام الحاسب الآلي إلا أنه عند الطعن على الحكم فان محكمة الاستئناف قد جاءت بتبرئة المتهمين وجاء في قرارها بأن المتهمين كان مخولان لهم بالدخول إلى نظام الحاسب الآلي وفقاً للمادة 17 /5 من القانون حتى وإن كان دخولهم لأغراض غير مشروعة.

ورغم ذلك فإن مجلس اللوردات الإنجليزي حين عرض عليه قضية أخرى (قضية المدعوة Ojomo) التي كانت تعمل محللة مالية حيث قامت بالدخول على جميع حسابات العملاء، وعلى الرغم أنها مخول ومصرح لها للدخول على بعض الحسابات، إلا أنها تمكنت من الحصول على معلومات سرية من هذه الحسابات وإعطائها إلى شخص آخر قام باستخدام تلك المعلومات والاستيلاء على مبالغ مالية كبيرة من الصراف الآلي،

[53] النوايسة، عبد الإله محمد سالم، مرجع سابق، ص (54-55).
[54] Bainbridge. D: Introduction to computer law, London 2000, fourth edition p.312.

وعند تقديمها للمحاكمة قررت محكمة الجزاء الابتدائية أن الفعل الذي قامت به (Ojomo) لا يشكل مخالفة لقانون إساءة استخدام الحاسب الآلي، لأنها كان لديها ترخيص بالدخول، وقد تم تأييد القرار من محكمة الاستئناف، وتم الطعن عليه لدي مجلس اللوردات الذي قرر أن سلوك (Ojomo) يشكل جريمة الدخول غير المصرح به وفقاً للمادة الأولى من قانون إساءة استخدام الحاسب الآلي، وذلك لأنها لم تحصل على التصريح اللازم للدخول لكل هذه المعلومات فالمادة 17/ 5 من قانون إساءة استخدام الحاسب الآلي تعني أن الدخول بتصريح إلى نوع معين من المعلومات لا يُعطي الصلاحية للدخول إلى معلومات أخرى، حتى وإن كانت من نفس النوع، وأكد مجلس اللوردات بأن قرار المحكمة في القضية لم يكن صحيحاً حيث فسرت المحكمة المادة 5/17 من القانون تفسيراً خاطئاً [55].

ومن خلال ما سبق نجد أن هناك بعض التشريعات التي نصت على حالة تجاوز حدود التصريح في النظام المعلوماتي قد ساوت بينها وبين من جريمة الدخول غير المشروع، والبعض الأخر مثل المشرع المصري قد جعلها جريمة مستقلة وأفرد لها نص خاص بها كما بينا سابقاً.

ونحن من جانبنا نؤيد ذلك الاتجاه الذي سلكه المشرع المصري وأن كنا نرى أنه من الأفضل ضبط صياغتها بإضافة تلك الحالة التي يكون مرتكبها موظف داخل مؤسسة النظام المعلوماتي بأن يكون تجريمها مشروط بوجود منع صراحة بموجب الأنظمة الداخلية للمؤسسة أو بموجب قرار مكتوب من قبل الجائز الشرعي للنظام المعلوماتي أو من الموظف الذي ينوب عنه كما فعل المشرع اليوناني وذلك لكون أن الفاعل في جريمة تجاوز حد التصريح غالباً ما يكون من العاملين لدى الجهة التي تم الدخول الي النظام المعلوماتي بها، كما يحفز ذلك الأمر كل الجهات على أن تحدد اختصاصات وتصريح الدخول لكل عامل بدقة مما يسهل معرفة حدوث تجاوز من عدمه.

الفرع الثاني: جريمة البقاء غير المصرح به في النظام المعلوماتي

يقصد بالبقاء غير المصرح به في النظام المعلوماتي بأنه التواجد داخل النظام المعلوماتي خلافًا لإرادة من له الحق في منح الإذن في التواجد في النظام المعلوماتي، وجاءت أهمية تجريم تلك الحالة لمواجهة عدة افتراضات وصور أهمها حالتين للبقاء غير المصرح به في النظام المعلوماتي:

[55] د/ الرواشدة، سامي، ود/ الهياجنة، أحمد، مرجع سابق، ص (149-150).

الحالة الأولى: كوجود تصريح للدخول إلى النظام المعلوماتي مرتبط بوقت محدد إلا أن هذا الوقت ينتهي ومع ذلك يظل الشخص داخل النظام المعلوماتي، فالبقاء في هذه الفرضية رغم علم الشخص بأن وجوده داخل النظام المعلوماتي غير مشروع يكون بذلك مرتكباً لجريمة البقاء غير المصرح به في النظام المعلوماتي.

الحالة الثانية: في الأحوال التي قد يكون فيها دخول الشخص إلى النظام المعلوماتي عن طريق الخطأ أو عن طريق الصدفة، دون قصد جنائي منه إلا أن الفاعل بعد اكتشافه ذلك الأمر وعلمه وإدراكه بأن دخوله إلى النظام المعلوماتي غير مشروع ومع ذلك يظل في النظام ولا يخرج منه، يكون بذلك مرتكباً لجريمة البقاء غير المصرح به في النظام المعلوماتي.

ففي الحالتين السابقتين لا يمكننا معاقبة الفاعل على بقائه في النظام من خلال نصوص جريمة الدخول غير المشروع وذلك لتوافر تصريح للدخول ابتداءً، ولعدم توافر العمد لدى الفاعل حال دخوله بالحالة الثانية من ناحية أخرى، ومن هنا جاءت الأهمية للنص على الجريمة.

ومن هنا يكون قد اتضح جلياً الفرق الجوهري بين جريمة الدخول غير المشروع إلى النظام المعلوماتي وجريمة البقاء غير المصرح به النظام المعلوماتي كون جريمة البقاء غير المصرح به النظام المعلوماتي تتميز بأنها جريمة مستمرة فالسلوك الإجرامي فيها يستمر مع تلك الاعتداءات على المصلحة القانونية التي يحميها المشرع وذلك منذ اللحظة التي يعلم الفاعل فيها أن دخوله إلى النظام المعلوماتي غير مشروع أو من اللحظة التي يدرك فيها أن التصريح الخاص به قد انتهى سواء أدى البقاء في النظام المعلوماتي إلى نتيجة معينة أم لا، وذلك بخلاف جريمة الدخول غير المشروع إلى النظام المعلوماتي كونها جريمة موقتة، كما أن جريمة الدخول غير المشروع جريمة إيجابية على خلاف الأمر في جريمة البقاء غير المصرح به النظام المعلوماتي التي تعتبر جريمة سلبية ترتبت بسلوك سلبي وهو عدم البقاء داخل النظام المعلوماتي [56].

ومن خلال البحث السالف بيانه بالمطلب السابق نجد أيضاً أن العديد من التشريعات العربية قد تناولت جريمة البقاء غير المصرح به في النظام المعلوماتي بجانب جريمة تجاوز حدود التصريح وبعدهم ساوى بينهما وبين جريمة الدخول غير المشروع ومن تلك التشريعات ما انتهجه المشرع الإماراتي في قانون مكافحة الشائعات والجرائم الإلكترونية وعاقب عليهما جميعاً كما بينا سابقاً وفق المادة (2) ضمن الجرائم الواقعة على تقنية المعلومات، وكذلك نهج ذات النهج المشرع العماني في قانون مكافحة جرائم تقنية المعلومات في

[56] الحمّادي، خالد سليمان عبد الله، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة، رسالة ماجستير، كلية القانون جامعة قطر، عام 2019م، ص (35-36).

المادة الثالثة، وأيضاً المشرع القطري في قانون مكافحة الجرائم الإلكترونية في مادته الثالثة في الفقرة الأولى، وسار أيضاً على ذات النهج المشرع الجزائري فساوى في المادة 394 مكرر من قانون العقوبات في التجريم بين فعل الدخول غير المشروع وبين البقاء في النظام المعلوماتي أو في جزء منه بالتحايل.

وأما عن المشرع السعودي في نظام مكافحة جرائم المعلوماتية، كما بينا سابقاً نجد أن المشرع السعودي أنه أقتصر على جريمة الدخول غير المشروع على حالة الجاني التي لا يتمتع بتصريح للدخول، وهو ما يعني كما أوضحنا أنه بذلك قد يفتح المجال لإباحة الطرق الأخرى وهروب الجاني من العدالة مثل تجاوز شروط الترخيص وحدود التصريح الخاص بالدخول إلى النظام المعلوماتي، أو البقاء بشكل غير مشروع عند وجود تصريح سابق أو الدخول عن طريق الخطأ أو الصدفة دون وجود القصد الجنائي إلا أن الجاني يقرر البقاء مع علمه وإدراكه بأن دخوله إلى النظام المعلوماتي أصبح غير مشروع، وقد وضحنا ذلك الأمر في المطلب السابق.

وصفوة القول الذي نراه جلياً في ذلك الأمر أن عدم النص على جريمة البقاء غير المصرح به في النظام المعلوماتي كجريمة مستقلة أو كجريمة مرتبطة بجريمة الدخول غير المشروع إلى النظام المعلوماتي يعتبر أمراً في غاية الخطورة ونقص تشريعي حاد يجب أن يتم سده بأقصى سرعة، إذ قد يؤدي ذل إلى إفلات الكثير من مجرمي الجرائم المعلوماتية من العقاب أو استغلال ذلك الفراغ التشريعي من أجل ارتكاب الجرائم المعلوماتية والهروب من العدالة وذلك لعدم إمكانية تطبيق عقوبة جريمة الدخول غير المشروع على العديد من الحالات كما بينا سابقاً.

وأما على صعيد التشريعات الأجنبية فنجد أن قانون العقوبات الفرنسي جرم في المادة 323-1 فعل الدخول أو البقاء بالتحايل في كل أو جزء من نظام المعالجة الآلية. [57] وكذا جُرم البقاء غير المصرح به بقانون العقوبات الإيطالي في المادة 615، وقانون العقوبات البلجيكي في المادة 525/ب.

الفرع الثالث: جريمة التنصت أو الالتقاط للمعلومات في النظام المعلوماتي

يقصد بالالتقاط أو التنصت أو الاعتراض غير المشروع للمعلومات في النظام المعلوماتي كما عرفه المشرع السعودي بنظام مكافحة جرائم المعلوماتية في المادة الأولى في الفقرة العاشرة بأنه "مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح"، ويتم الاعتراض أو الالتقاط باستخدام وسائل تقنية عن طريق

[57] Article 323-1 Modifie par LOI n°2012- 410-du 27 mars 2012- art. 9 Le fait d'accederou de se maintenir, frauduleusement, dans tout oupartie d'un systè mede traitementautomatise de donnéesestpuni de deuxansd' emprisonnement ET de 30000 euros d'amende.

التقاط الانبعاثات الكهرومغناطيسية الناتجة عن نظام معلوماتي أو حاسب آلي ولا تعتبر تلك الانبعاثات الكهرومغناطيسية بيانات، ومع ذلك يمكن إعادة بنائها واستقبالها بصورة بيانات ومعلومات. [58]

ولبيان أوجه الشبه والاختلاف بين جريمة الدخول غير المصرح به، وبين جريمة الاعتراض أو التنصت أو الالتقاط للمعلومات في النظام المعلوماتي، سنستعرضها كالآتي: [59]

أولاً: أوجه التشابه بين الجريمتين:

- تتشابه الجريمتين في أنهما يؤديان إلى نتيجة واحدة، وهي الوصول إلى معلومات وبيانات غير مصرح للفاعل الوصول إليها ويصل اليها بطريقة غير مشروعة.
- كما أنهما يتفقان في أنه يشترط لتجريمهما عدم وجود تصريح لدى الجاني ممن يملك الحق بذلك؛ فلا يتصور وقوعهما إذا توافر ذلك التصريح ممن له الحق بذلك.
- كما أنهما وطبيعة الحالية يشترط لوقوعهما توافر العمدية أو القصد الجنائي، أي أنهما لا ترتكبان بطريق الخطأ.

ثانياً: أوجه الاختلاف بين الجريمتين:

- جريمة الاعتراض أو التنصت أو الالتقاط للمعلومات في النظام المعلوماتي لا تتطلب الدخول إلى النظام المعلوماتي، بل أنها مجرد تلصص على رسائل أو معلومات أو بيانات بين جهازين ولا يستطع الجاني فيها اختيار المعلومات أو البيانات بل يلتقط كل ما يرسل.
- كما أن جريمة الدخول غير المشروع يفترض فيها تشغيل النظام المعلوماتي، أما جريمة الاعتراض غير المشروع يفترض فيها تشغيل النظام المعلوماتي من طرف أخر.
- يختلفان أيضاً في الطبيعة القانونية فجريمة الدخول غير المشروع في الأغلب جريمة شكلية وقتية، أما جريمة الاعتراض غير المشروع هي جريمة لا تقع إلا بعد تحقق نتيجة التقاط الانبعاثات الكهرومغناطيسية كما أنها جريمة مستمرة مع استمرار فعل الاعتراض.

[58] عبد اللاه، هلالي، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقاتها في النظام البحريني، ط2013، ص (255).
[59] النوايسة، عبد الإله محمد سالم، مرجع سابق، ص (61-62).

ولقد اهتم المشرع السعودي بتجريم جريمة التنصت أو الالتقاط للمعلومات في النظام المعلوماتي لفرض حمايته القانونية للحق في الاتصالات الأمنة وحماية حرمة البيانات والمعلومات التي تنتقل عبر النظام المعلوماتي فجريمة الالتقاط للمعلومات في النظام المعلوماتي تعد انتهاكاً صارخاً للحق في الاتصالات الأمنة ومنع التنصت والتلصص عليها.

كما أن المشرع العربي لم يكن بمنأى عن تجريم جريمة الالتقاط للمعلومات في النظام المعلوماتي نظراً لما تشمله من خطورة بالغة على المعلومات المرسلة عبر النظام المعلوماتي سوء على مستوى الفرد أو المؤسسات أو الدولة. ومن خلال البحث بالتشريعات العربية كما اعتدنا نجد اهتمام بالغاً من العديد من التشريعات العربية فقد تناولت معظمهم جريمة الاعتراض أو التنصت أو الالتقاط غير المشروع للمعلومات كجريمة مستقلة.

ومن تلك التشريعات المشرع الإماراتي حين عرف الاعتراض في قانون مكافحة الشائعات والجرائم الإلكترونية بأنه "مشاهدة أو مراقبة البيانات أو المعلومات أو الحصول عليها بغرض التنصت أو التعطيل، أو التخزين أو النسخ أو التسجيل أو التحايل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق". ونص المشرع الإماراتي على عقوبة الاعتراض غير المشروع وإفشاء المعلومات في المادة 12 على أنه "يعاقب بالحبس والغرامة التي لا تقل عن مائة وخمسون ألف درهماً ولا تزيد على خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من أعاق أو اعترض الوصول إلى شبكة معلوماتية أو موقع إلكتروني أو نظام معلومات إلكتروني أو أي اتصال أو معلومات أو معلومات أو بيانات إلكترونية."

أما المشرع عن المشرع الأردني في قانون الجرائم الإلكترونية الأردني، فقد عاقب عن جريمة الالتقاط غير المشروع في المادة (7) الفقرة (أ) من القانون ونص على أنه "يعاقب كل من قام قصداً ودون وجه حق باعتراض خط سير البيانات أو التقاط محتواها أو اعاق أو حور أو شطب أو قام بتسجيل ذلك المحتوي سواء المرسل عن طريق الشبكة المعلوماتية أو تقنية المعلومات أو نظام المعلومات أو البيانات المتبادلة داخل النظام أو الشبكة ذاتها بالحبس مدة لا تقل عن ثلاثة ستة أشهر وبغرامة لا تقل عن ألف وخمسمائة دينار ولا تزيد على ستة آلاف دينار".

وكذلك نهج ذات النهج المشرع القطري في القانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية وعرف الالتقاط بأنه "مشاهدة البيانات أو المعلومات الإلكترونية أو الحصول عليها". وفي مادته

الرابعة حيث نص على" يعاقب بالحبس مدة لا تجاوز سنتين، وبالغرامة التي لا تزيد عن مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من التقط أو اعترض أو تنصت عمداً، دون وجه حق، على أية بيانات مرسلة عبر الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، أو على بيانات المرور".

وأما المشرع العماني في المرسوم السلطاني رقم 12/ 2011 بإصدار قانون مكافحة جرائم تقنية المعلومات لم يخالف ذات النهج الذي انتهجته معظم التشريعات العربية واتفق في تعريف الالتقاط مع التعريف القطري، وفي مادته الثامنة نص على "يعاقب بالسجن مدة لا تقل عن شهر ولا تزيد على سنة وبغرامة لا تقل عن خمسمائة ريال عماني ولا تزيد على ألفي ريال عماني، أو بإحدى هاتين العقوبتين، كل من اعترض عمداً ودون وجه حق باستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو تنصت عليها".

وأما المشرع الكويتي في القانون رقم 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات عندما عرف مفهوم الالتقاط المعلوماتي عرفه بأنه "مشاهدة البيانات أو المعلومات الواردة في أي رسالة إلكترونية أو سماعها أو الحصول عليها، ويشمل ذلك المنقولة الكترونياً". وفي مادته الرابعة نص المشرع الكويتي في الفقرة الثالثة بالمعاقبة بالحبس مدة لا تجاوز سنتين وبغرامة لا تقل عن ألفي دينار ولا تتجاوز خمسة آلاف دينار أو بإحدى هاتين العقوبيين كل من "تنصت أو التقط أو اعترض عمداً، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات". وتزداد العقوبة في حالة قيام الجاني بإفشاء ما توصل إليه من معلومات أو بيانات نتيجة اعتراضه أو التقاطه أو تصنته عليها، للحبس مدة لا تتجاوز ثلاث سنوات وبغرامة لا تقل عن ثلاثة آلاف دينار ولا تتجاوز عشرة آلاف دينار أو بإحدى هاتين العقوبيين.

ومن التشريعات العربية الأخرى التي تناولت جريمة الاعتراض أو التنصت أو الالتقاط للمعلومات في النظام المعلوماتي نجد أن المشرع المصري في القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات عرف الاعتراض بأنه "مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق". كما نصت المادة (16) من قانون مكافحة جرائم تقنية المعلومات على أنه "يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف ولا تتجاوز مائتين وخمسون ألف جنية، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها".

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

وأما عن المشرع السعودي في نظام مكافحة جرائم المعلوماتية، كما بينا سابقاً فقد عرف الالتقاط بأنه مشاهدة البيانات، أو الحصول عليها دون مسوغ نظامي صحيح. وقد جرم المشرع السعودي في المادة الثالثة في الفقرة الأولى جريمة الاعتراض أو التنصت أو الالتقاط للمعلومات في النظام المعلوماتي وعاقب عليها بالسجن مدة لا تزيد عن سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبيين، لكل شخص يرتكب "التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي -دون مسوغ نظامي صحيح-أو التقاطه أو اعتراضه".

وأما على صعيد التشريعات الأجنبية فنجد أيضاً الاهتمام البالغ لجريمة جريمة الاعتراض أو التنصت أو الالتقاط للمعلومات في النظام المعلوماتي وخاصة تجريم الاعتراض القصدي للانبعاثات الكهرومغناطيسية، فنجد المادة الثالثة من الاتفاقية الأوروبية لجرائم الإنترنت لعام 2001م. تدعو الدول الأطراف ضرورة تجريم الاعتراض القصدي للانبعاثات الكهرومغناطيسية (Electromagnetic emissions) الصادرة عن أجهزة الحاسب الآلي، وكذلك جرمت العديد من التشريعات الاعتراض غير القانوني بشكل مستقل عن جريمة الدخول غير المشروع إلى النظام المعلوماتي ومنها قانون جرائم الإنترنت البرتغالي (Law No. 15, 2009 of September 109/2009حيث جاءت المادة السابعة من القانون تحت عنوان الاعتراض غير القانوني وجرمت هذه المادة القيام بالاعتراض دون إذن قانوني أو تصريح من المالك أو الحائز الذي يكون كامل النظام أو جزء منه تحت إشرافه بأي وسيلة تقنية للمعلومات المنقولة من شبكة الحاسب الآلي أو إليه أو بوساطته، كما ذهبت بعض التشريعات إلى تجريم الشروع في جريمة الاعتراض، بل وتجاوز ذلك لتجريم تصنيع وبيع الأدوات والآلات التي تستخدم في ارتكاب هذه الجريمة مثل المشرع البرتغالي في المادة (7-2 و3) وجرم أيضاً قانون العقوبات الكندي كل فعل يقوم به الشخص من اعتراض أو يتسبب في اعتراض بدون وجه حق أو بالتحايل بأي وسيلة إلكترونية أو ميكانيكية أو سمعية أو غيرها بشكل مباشر أو غير مباشر أي وظيفة من وظائف الكمبيوتر [60] .

الخاتمة

ركزت الدراسة على الجهود الدولية والعربية المبذولة لمكافحة الجرائم المعلوماتية من خلال تسليط الضوء على أهم الاتفاقيات الدولة والعربية التي تصب اهتمامها على مكافحة جريمة الدخول غير المشروع إلى النظام

[60] النوايسة، عبد الإله محمد سالم، مرجع سابق، ص (59-60).

المعلوماتي، كما اهتمت الدراسة ببيان جهود المملكة العربية السعودي في مكافحة الجرائم المعلوماتية في العموم وبيان مدى تطور جهودها في مكافحة جريمة الدخول غير المشروع إلى النظام المعلوماتي على وجه الخصوص على المستويين المستوى الحكومي ومستوى القطاع الخاص، كما تعمقت الدراسة في التعريف بجريمة الدخول غير المشروع إلى النظام المعلوماتي من عدة نواحي، حيث اهتمت الدراسة في التعريف بجريمة الدخول غير المشروع من الناحية اللغوية ثم سلطت الضوء على اختلاف الفقهاء القانونين في محاولاتهم لوضع تعريف محدد وشامل لجريمة الدخول غير المشروع وصولاً إلى التعريف النظامي لجريمة الدخول غير المشروع في نظام مكافحة جرائم المعلوماتية السعودي وما يماثلها من تشريعات ونظم قانونية تجرم فعل الدخول غير المشروع إلى النظام المعلوماتي، ثم ختمت الدراسة ببيان أوجه التشابه والاختلاف بين جريمة الدخول غير المشروع إلى النظام المعلوماتي وما يشابها أو يرتبط بها وبيان أوجه التشابه والاختلاف بينهم.

وقد خرجت الدراسة بالعديد من النتائج والتوصيات أهمها ما يلي:

1. المملكة العربية السعودية بذلت في سبيل مكافحة الجرائم المعلوماتية جهداً مكثفاً فقامت بتطوير النظم التشريعية وكذلك إنشاء هيئة الاتصالات وتقنية المعلومات لمواكبة سبل مكافحة كافة الجرائم المعلوماتية.
2. لم يتفق الفقهاء على تعريف موحد للجريمة المعلوماتية أو جريمة الدخول غير المشروع إلى النظام المعلوماتي.
3. اعتمد النظام السعودي في تعريفه للجريمة المعلوماتية على معيار الوسيلة التي ترتكب بها الجرائم المعلوماتية أكثر من محل الجريمة فاهتم بتعرف المقصود بالشبكة المعلوماتية والحاسب الآلي كوسيلة لارتكاب الجرائم المعلوماتية.
4. أن المشرع السعودي في تعريفه لجريمة الدخول غير المشروع قد اقتصر في التعريف على حالة الجاني التي لا يتمتع بتصريح للدخول، وهو ما يعني فتح المجال لإباحة باقي الطرق والحالات على سبيل المثال حالة تجاوز شروط الترخيص، أو البقاء بشكل غير مشروع عند وجود تصريح سابق، مما نوصي معه بتعديلها لتشمل كافة صور الدخول غير المشروع.

5. أن المشرع السعودي قد اقتصر على حالة الدخول العمدي وبالتالي أباح الدخول غير العمدي عن طريق الخطأ مما نوصي بتعديل ذلك التعريف حتى يشمل حالة الدخول العمدي وكذلك حالة الدخول بخطأ غير عمدي والبقاء بدون وجه حق.
6. أن عدم النص على جريمة البقاء غير المصرح به في النظام المعلوماتي يعتبر أمراً في غاية الخطورة ونقص تشريعي حاد يجب أن يتم سده بأقصى سرعة أما باعتبارها جريمة مستقلة أو كجريمة مرتبطة بجريمة الدخول غير المشروع إلى النظام المعلوماتي.
7. تميز المشرع السعودي عن العديد من التشريعات المماثلة في كونه لم يشترط لقيام جريمة الدخول غير المشروع أن يكون النظام المعلوماتي أو الحاسب الآلي، أو الموقع الإلكتروني محمي بحظر الدخول عليه بكلمة سر مثلاً، بل أعتبر الدخول غير المشروع معاقب عليه حتى ولو لم يعني صاحبه أن يحميه من تطفل الأخرين طالما توافرت أركان الجريمة والقصد الجنائي.

المراجع

- الصاعدي، محمد، "جرائم الإنترنت وجهود المملكة العربية السعودية في مكافحتها." في أعمال ندوات: مكافحة الجريمة عبر الإنترنت – ورشة عمل: أمن المعلومات والتوقيع الإلكتروني، القاهرة: المنظمة العربية للتنمية الإدارية، (2010م).
- Goshua (B.hill), nancy (E. MARION), Introduction to Cybercrime: Computer Crimes Laws, and Policing in the 21st Century, PUBLISHED IN PRAEGER SECURITY INTERNATIONAL, USE, 2016.
- المراغي، أحمد عبد اللاه، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها –دراسة تحليلية تأصيلية مقارنة -بحث مُقدَم إلى المؤتمر العلمي العاشر لكلية الحقوق جامعة أسيوط، عنوان المؤتمر (العصر الرقمي واشكالياته القانونية)، في الفترة من 5-6 أبريل لسنة 2016م).
- المطيري، خالد ظاهر محمد، مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية، (الكويت: أكاديمية سعد العبد الله للعلوم الأمنية، 2020م).

- الغياثين، محمد حمد عمر، الجرائم المعلوماتية عابرة الحدود-دراسة مقارنة-قدمت لنيل درجة الدكتوراه في كلية الحقوق جامعة القاهرة، عام (2013م).
- د/ القاضي، رامي متولي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، الطبعة الأولي، عام 2011.
- الجنبيهي، منير محمد، والجنبيهي، ممدوح محمد، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي، الاسكندرية، عام 2005م.
- الأمين، محمد، وعبد الحميد، محسن، معاير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة، اكاديمية نايف العربية للعلوم الأمنية، الرياض ط1، عام 1998م.
- حسام، محمد، ولطفي، محمود، الحماية القانونية لبرامج الحاسب الإلكتروني، دار الثقافة للطباعة والنشر القاهرة ط1، عام 1978م.
- الدعجة، أمجد حسن مرشد، استراتيجية مكافحة الجرائم المعلوماتية، جامعة أم درمان، السودان، رسالة ماجستير، عام 2014م.
- عبد الحفيظ، أيمن، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة بأكاديمية مبارك، العدد الخمس والعشرون، يناير 2004م.
- عبد اللاه، هلالي، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها أ.د. هلالي عبده اللاه أحمد، أستاذ القانون الجنائي كلية الحقوق، جامعة أسيوط، القاهرة دار النهضة العربية، 2011م.
- د: عبد الرازق، رانا مصباح عبد المحسن (أستاذ القانون الجنائي المساعد بقسم القانون – الكلية التطبيقية-جامعة الأميرة نورة بنت عبد الرحمن)، آليات مكافحة الجرائم السبرانية في المملكة العربية السعودية "دراسة تحليلية" المجلة القانونية (مجلة متخصصة في الدراسات القانونية)، " ISSN: 2537 – 0758".
- النوايسة، عبد الإله محمد سالم، جريمة الدخول غير المشروع في تشريعات الجرائم الإلكترونية العربية: دراسة مقارنة، المجلة القانونية والقضائية، مركز الدراسات القانونية والقضائية، وزارة العدل، قطر، ع 1، س 10، عام (2016).

- د: حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في الجرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، القاهرة، عام (2004).
- د: البشري، محمد الأمين، التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات العربية المتحدة، عام (2000).
- أبن منظور، لسان العرب، دار أحياء التراث العربي، بيروت، عام (1419هـ)، (ج12 / 92).
- العامري، سليمان بن إبراهيم بن أمان، جريمة الدخول غير المشروع على المواقع الإلكترونية المتعلقة بأمن الدولة: دراسة تأصيلية تطبيقية في النظام السعودي، المجلة الأكاديمية للأبحاث والنشر العلمي، الإصدار الرابع والأربعون، تاريخ الإصدار 5-12-2022م.
- الجوهري، إسماعيل بن حماء، معجم الوسيط، دار المعرفة بيروت، ط 6 (عام 1435هـ).
- د: القطري، محمد نصر محمد، الإشكاليات القانونية لحماية سلامة المعلومات: دراسة تطبيقية على الحماية الجنائية من الإتلاف المعلوماتي، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، مج 24، ع 93، إبريل 2015م.
- العبيدي، أسامة غانم، جريمة الدخول غير المشروع إلى النظام المعلوماتي: دراسة قانونية في ضوء القوانين المقارنة، مجلة دراسات المعلومات، ع 14، مايو 2012م.
- بوزيدي، مختارية، ماهية الجريمة الإلكترونية، بحث مقدم في الملتقي الوطني: أليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر،2017/3/29م.
- ناصر، حمودي، الحماية الجنائية للتجارة الإلكترونية، رسالة ماجستير، جامعة الجزائر، عام 2015م.
- Orin S. Kerr: Cybercrime’s Scope: Interpreting (Access) and Authorization NYU Law Review, Vol. 78, No. 5, pp. 1596-1668, November 2003.
- د: نصر أحمد، شريف، الجوانب الموضوعية لجرائم الدخول غير المشروع إلى الأنظمة المعلوماتية: دراسة مقارنة، مجلة كلية الشريعة والقانون بطنطا، العدد الخامس والثلاثون، يونيو 2020م.

- Dr: Rizgar Kadir, International Solution, 27Tex.Int. L.J. (l992). P496- 497, Shackelford. S: Computer- Related Sharia & Law, IssueNo.40-October 2009, p. 56.
- د: عطا الله، شيماء عبد الغني، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، جامعة المنصورة، كلية الحقوق عام2005.
- المعجم الوسيط، الصادر عن مجمع اللغة العربية، بمصر، ط 1381هـ، 1961 م، ج2.
- المناصير، حسن فضيل خليف، وربيع، عماد محمد أحمد، جريمة الدخول غير المشروع إلى النظام المعلوماتي والتعدي على محتوياته: دراسة مقارنة، رسالة ماجستير، جامعة جريش، الأردن، عام 2016م.
- حسين، أحمد حسين، وربيع، نظم المعلومات المحاسبية، الإطار الفكري والنظم التطبيقية، مكتبة الإشعاع الفنية، القاهرة، 1998م.
- أ/ عباوي، نجاة، الإشكاليات القانونية في تجريم الاعتداء على أنظمة المعلومات، مجلة دراسات المعلومات، ع 14، مايو2012م.
- د/ الرواشدة، سامي، ود/ الهياجنة، أحمد، مكافحة الجريمة المعلوماتية بالتجريم والعقاب: القانون الإنجليزي نموذجاً، المجلة الأردنية في القانون والعلوم والسياسة، مج 1، ع3، عام 2009م.
- خليفة، محمد مسعود محمد، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، رسالة مقدمة للحصول على درجة الماجستير في الحقوق، كلية الحقوق، جامعة الإسكندرية، عام 2006-2005.
- Bainbridge. D: Introduction to computer law, fourth edition, London 2000.
- الحمّادي، خالد سليمان عبد الله، جريمة الدخول غير المشروع إلى النظام المعلوماتي في القانون القطري: دراسة مقارنة، رسالة ماجستير، كلية القانون جامعة قطر، عام 2019م.
- د: عبد اللاه، هلالي، جرائم المعلوماتية التقليدية والمستحدثة وتطبيقاتها في النظام البحريني، ط2013، ص (255).